

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

System Hardware Requirements

ODIN

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

Contents

1	Revision History	3
2	Definitions and Acronyms	3
3	References	3
4	Purpose	4
5	Hardware Requirements	5
5.1	Disk Size Requirements	5
5.2	Disk Encryption (LUKS) Requirements	6
5.3	NIDS Option Requirements	6
5.4	Recording Option Requirements	6
6	GFE Requirements	7
6.1	GFE for test/integration	7
7	Interface Requirements	8
7.1	Operating System Requirements	8
8	Other information	9
9	ODIN Log Concentrator	10
9.1	Hardware Requirements	10

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

1 Revision History

Issue	Date	Author	Changes
1.0	2015-04-02	Magnus Juntti	First version
1.4	2015-09-14	Magnus Juntti	Changed disk size recommendations
1.5	2015-10-02	Magnus Juntti	Changed title to hardware requirements
1.6	2015-10-21	Magnus Juntti	Changed syslog RFC. Updated text about odin-tunnel.
1.7	2016-01-15	Magnus Juntti	Added NIDS Option requirements
1.8	2016-01-30	Magnus Juntti	Increased memory requirements for NIDS
1.9	2018-06-06	Magnus Juntti	Changed disk size requirements
1.10	2018-12-04	Magnus Juntti	Changed disk size requirements
1.11	2019-10-24	Magnus Juntti	Changed disk size requirements
2.0	2020-03-24	Magnus Juntti	Changed text to ODIN 2.0 specifications
2.1	2021-12-01	Magnus Juntti	Corrected a typo.
2.2	2022-05-31	Magnus Juntti	Added LUKS requirements

2 Definitions and Acronyms

Definition	Description
GFE	Government Furnished Equipment
TAK	Totalförsvarets Aktiva Kort
TEID	Totalförsvarets Elektroniska ID
CPU	Central Processing Unit
RAID	Redundant Array of Inexpensive Disks
GB	GigaByte
RAM	Random Access Memory
HIDS	Host Intrusion Detection System
TPM	Trusted Platform Module

3 References

ID	Document ID	Title
1	ICD-ODIN-002	Log Formats and Communication Interfaces

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

4 Purpose

This document defines the system requirements for running the software package ODIN Security Log and its options.

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

5 Hardware Requirements

Server/Workstation with the following minimum requirements:

- Compatible with CentOS 7.9 or later in version 7-branch of CentOS.
- Minimum 4 CPU-cores with multithreading, minimum 2GHz/core, Recommended 8 CPU-cores with multithreading, 2.5GHz/core
- Minimum 32GB RAM, Recommended 96GB RAM
- Display with at least 1280*1024 pixels, recommended minimum 1920x1080. The log-analysis becomes more usable the larger the screen and resolution.
- Minimum storage size 160GB based on normal log flow. If the system has excessive logging larger drives may be needed. This depends on organizational requirements. See separate chapter for size calculations.
- Use fast drives, NVMe, SSD or 10-15k SAS mechanical disks are preferred.
- Redundant power units
- DVD-RW-unit for log-backup
- Minimum 1 Ethernet-port, fiber or TP
- For smartcard support, Avenra NetID smartcards are supported out-of-the-box

For the alert function using a USB-relay, the following USB-relay shall be used:

- KMTronic USB-relay with one port (Model: U1CRB, USB one relay)

For unidirectional connection of ODIN to several security domains, the following extra hardware is also required:

- Network diode on each connection
- Switch to connect all incoming domains into one connection to ODIN

5.1 Disk Size Requirements

Disk sizes shall be chosen depending on two main factors:

1. Time between archiving
2. History time in analysis tool, i.e. how long is the searchable interval in the indexed database that is used for log analysis.

ODIN comes with a predefined disk partitioning that this calculation is based on. The customer may choose to alter this partitioning and thus this calculation may be different.

Choose sizes according to:

80 GB + the largest number of the following (all sizes in GB):

1. $(\text{Log amount per day} + (\text{days between archiving} * (0,1 * \text{log amount per day}))) / 0,25$

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

2. Days of history * 0,5 * Log amount per day

Example: If you have 2 GB of logs per day, you want to be able to analyze logs 60 days back in time and you archive logs every 30 days, the calculations would be:

1. $80 + (2 + (30 * (0,1 * 2))) / 0,25 = 112 \text{ GB}$

2. $80 + 60 * 0,5 * 2 = 140 \text{ GB}$

Thus you would choose 140 GB of storage for your ODIN.

5.2 Disk Encryption (LUKS) Requirements

To use disk encryption, the hardware must have a TPM 2.0 compatible module and this must be enabled in BIOS.

5.3 NIDS Option Requirements

If the NIDS option is chosen, the following requirements replace the corresponding requirements above:

- Core-requirement is as above but also one extra core for each network interface that is running NIDS
- Minimum memory requirement increases with 2GB per NIDS-interface
- 1 Ethernet-port, fiber or TP for logging (shall be the first enumerated NIC)
- 1 Ethernet-port, fiber or TP for each NIDS-interface that shall be used

5.4 Recording Option Requirements

If the Recording Option is chosen (with NIDS), the following requirements replace the corresponding requirements above:

- Extra disk space, the size of the expected network traffic per day times the number of days recording shall be saved. For example, if you have 10 GB network traffic per day (summary of all recorded interfaces) and want to save 30 days, the extra amount would be 300 GB.

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

6 GFE Requirements

In case special cryptographic components are needed for government/military installations, these products can be integrated with ODIN provided that they are compatible with CentOS 7 or RHEL 7.

These products are considered GFE and must be provided by the purchaser.

For Sweden the following GFE-products apply to ODIN and are compatible with ODIN:

- KrAPI for handling of Swedish Armed Forces smartcards (TAK/TEID).

6.1 GFE for test/integration

Special authentication solutions such as GFE smartcards require that such smartcards and readers compatible with the smartcard are provided as GFE for use during test/integration. Such equipment will be returned when test/integration is complete.

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

7 Interface Requirements

- Time synchronization use NTP according to RFC 5905. NTP can be configured in standard mode or broadcast/multicast if used on a unidirectional link.
- Log/IDS-interfaces according to ref [1].

7.1 Operating System Requirements

For maximal use of ODIN, the software ODIN Integrity shall be installed in all supervised nodes. ODIN Integrity is compatible with most Operating Systems on the market such as Windows and Linux based systems. If HIDS-use is not wanted and ODIN is only used for log handling, all syslog compliant units can use syslog and ODIN can analyze these logs by creating log patterns for them. For Windows-based systems it is **STRONGLY** recommended that ODIN Logcollector is used to transfer logs and not any other third-party syslog-compliant tool.

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

8 Other information

ODIN requires customization to the log formats generated by the system by creating pattern files for manual and automatic log analysis tools. This is a service that can be purchased as an option or performed by the purchaser using the supplied manuals.

Supervision of the server can be performed using the program odin-heartbeat which is supplied with ODIN. This will generate a security alarm if the communication with the supervised system fails.

If ODIN Log Concentrator (see chapter 9) is used for unidirectional links, encryption of the communication can be performed using odin-tunnel which is based on OpenSSL crypto-lib with using an AES 256 CBC symmetric crypto with a pre-shared key. It is also possible to use odin-tunnel as a separate software if ODIN Log Concentrator is not used. Odin-tunnel has been tested on CentOS 6, 7, ubuntu, Solaris and Windows 7, 10 clients and Windows server 2012 and 2016.

Issued by Magnus Juntti	Document no. REQ-ODIN-001	Classification Unclassified
Approved by Magnus Juntti	Issue 2.2	Date 2022-05-31

9 ODIN Log Concentrator

This chapter defines the requirements on the optional ODIN Log Concentrator which can be used to integrate ODIN Security Log in a multi-level security domain where ODIN Security Log is connected via network diodes.

9.1 Hardware Requirements

Server with the following minimum requirements:

- Compatible with CentOS 7.7 or later in version 7-branch of CentOS.
- 2 CPU-cores, minimum 2GHz/core
- 8 GB RAM
- Hardware-RAID in RAID-1 configuration with minimum 2 drives
- Minimum Hard-drive size 80GB/drive
- Redundant power units
- No display is needed
- 2 Ethernet-ports, fiber or TP depending on interfaces used in the system/network diodes/ODIN