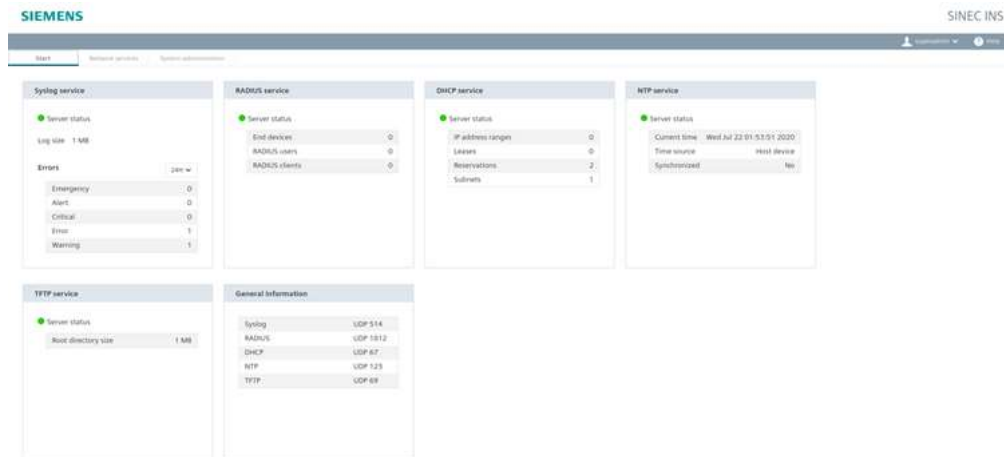Entry type: **Product note**, Entry ID: **109781021**, Entry date: **07/27/2020**

Sales and delivery release for the new network services SINEC INS V1.0

Sales and delivery release for the new network services SINEC INS V1.0

The new SINEC INS V1.0 network services are released for sale and delivery with immediate effect.

Product description

The software SINEC INS (Infrastructure Network Services) is a web-based application that combines various network services in one tool. This simplifies installation and administration of all network services relevant for industrial networks. SINEC INS is a central and scalable infrastructure server on which the network services can be adapted to different system sizes as required. The various network services provide support in industrial plants, for example to authenticate devices or users in an industrial network. As a Syslog server, SINEC INS can receive Syslog messages from devices or other Syslog clients in the network as well as forward Syslog messages received as Syslog relays to other Syslog servers or Security Information and Event Management (SIEM) systems. In order to achieve temporal transparency, it is necessary to synchronize the system times in the industrial plants as well via Network Time Protocol. By using SINEC INS as a DHCP server, it is possible to assign IP addresses to devices in the network and to configure additional parameters using options. Also featured is role-based user administration, which establishes a connection to a central UMC server. This enables the use of user data from a directory service.

Main features:

Syslog Server (including Secure Syslog)

- Receipt of Syslog messages from devices
- Save, display, sort and filter for a quick overview
- Supports the standardized formats RFC 3164 and RFC 5424
- Forwarding of Syslog messages to SIEM systems in RFC 5424 format for further analysis

RADIUS Server (Remote Authentication Dial-in User Services)

- User and device authentication in industrial networks
- Forwarding of device authentication to superimposed Network Access Control systems
- Device authentication via MAC addresses

DHCP Server (IP V4)

- Managing IP addresses
- Provision of additional options for DHCP clients: For example, host name, TFTP server address, path to the configuration file, etc.

NTP Server (including Secure Network Time Protocol)

- Time synchronization for all network devices in the industrial network

TFTP Server (Trivial File Transfer Protocol)

- Provision of firmware upgrade files and configuration files, for example

User management:

- Central administration of roles and rights for all SINEC INS network services
- Use of users from UMC or locally created users

Ordering data

Product (DVD):

Product name	Functions	Order number
SINEC INS V1.0 50 (DVD)	Network services for 50 Ethernet devices	6GK8751-1BA01-0BA0
SINEC INS V1.0 100 (DVD)	Network services for 100 Ethernet devices	6GK8751-1DA01-0BA0
SINEC INS V1.0 250 (DVD)	Network services for 250 Ethernet devices	6GK8751-1JA01-0BA0
SINEC INS V1.0 500 (DVD)	Network services for 500 Ethernet devices	6GK8751-1TA01-0BA0
SINEC INS V1.0 1000 (DVD)	Network services for 1000 Ethernet devices	6GK8751-1UA01-0BA0
SINEC INS V1.0 5000 (DVD)	Network services for 5000 Ethernet devices	6GK8751-1XA01-0BA0

Product (Online Software Delivery):

Product name	Functions	Order number
SINEC INS V1.0 50 (Download)	Network services for 50 Ethernet devices	6GK8751-1BA01-0BK0
SINEC INS V1.0 100 (Download)	Network services for 100 Ethernet devices	6GK8751-1DA01-0BK0
SINEC INS V1.0 250 (Download)	Network services for 250 Ethernet devices	6GK8751-1JA01-0BK0
SINEC INS V1.0 500 (Download)	Network services for 500 Ethernet devices	6GK8751-1TA01-0BK0
SINEC INS V1.0 1000 (Download)	Network services for 1000 Ethernet devices	6GK8751-1UA01-0BK0
SINEC INS V1.0 5000 (Download)	Network services for 5000 Ethernet devices	6GK8751-1XA01-0BK0

Note on Online Software Delivery (OSD) type of delivery:

The Online Software Delivery type of delivery is not available in all countries.

More information on Online Software Delivery: > 109759444

SUS:

Product name	Functions	Order number
SINEC INS 50 SUS	Software updates and software upgrades for 50 devices/per year	6GK8751-1BA01-0BL6
SINEC INS 100 SUS	Software updates and software upgrades for 100 devices/per year	6GK8751-1DA01-0BL6
SINEC INS 250 SUS	Software updates and software upgrades for 250 devices/per year	6GK8751-1JA01-0BL6
SINEC INS 500 SUS	Software updates and software upgrades for 500 devices/per year	6GK8751-1TA01-0BL6
SINEC INS 1000 SUS	Software updates and software upgrades for 1000 devices / per year	6GK8751-1UA01-0BL6
SINEC INS 5000 SUS	Software updates and software upgrades for 5000 devices/ per year	6GK8751-1XA01-0BL6

Hardware requirements:

Depending on the number of nodes used, the following hardware requirements apply:

Component	Up to 500 nodes	Up to 5000 nodes	More than 5000 nodes
Processor	2 cores with 2.16 GHz x64	2 cores with 2.6 GHz x64	4 cores with 3.6 GHz x64
RAM	2 GB	8 GB	16 GB
Hard disk space	128 GB HDD	256 GB SSD	512 GB SSD

Software requirements:

The following requirements apply to the software to be used:

Operating system	• Linux Ubuntu 18.04.2 LTS Desktop (64-bit) • Linux Ubuntu 18.04.2 LTS Server (64-bit) • SIMATIC OS V1.3 • RX1500 APE 1808 Debian 9.6.0
Supported operating system languages	• German • English
Web browser	• Google Chrome 67.0 or later • Firefox 60.0 or later • Microsoft Edge 83 or later • Internet Explorer 11.0 *)

Screen resolution	1920 x 1080 pixels (resizable)
Recommended virtualization platforms	● VMware Workstation Pro / VMware Workstation Player 15.0 ● Oracle VirtualBox 6.0 You can find additional information in the section below.

* The web browser is only supported to a limited extent

Additional notes:

Please note the installation and usage notes in the following file.

German: 🔲 ♂ Liesmich.htm (58.6 KB)

English: 🔲 ♂ Readme.htm (60.3 KB)

Additional information:

Website: ↗ http://www.siemens.com/sinec-ins

Software trial version:

You can find a trial version of the SINEC INS V1.0 product for 10 nodes with the following link: › 109781022

Security information

In order to protect technical infrastructures, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art IT security concept. Siemens' products and solutions constitute one element of such a concept. For more information about cyber security, please visit

https://www.siemens.com/cybersecurity#Ouraspiration.