



SynapSense Software

Installation Manual

Copyright © 2017 Panduit Corp. All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from Panduit. No patent liability is assumed with respect to the use of the information contained herein.

Although every precaution has been taken in the preparation of this book, Panduit assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Table of Contents

Overview	4
Panduit Technical Support	4
Severity 1 & 2 Issues:	4
Severity 3 & 4 Issues, Email - normal business hours:	4
Minimum System Requirements	5
Server Hardware	5
Server Software	5
Client PC	5
Preparing for Installation	6
Static IP Address Allocation	6
Setup for SynapSense Gateways	6
Setup for SynapSense Environment Server	6
Configure TCP and UDP Ports	6
Disable Anti-Virus Software	8
Disable Admin Approval Mode	8
SynapSense Installation	9
Installing MapSense Separately	11
Configure Optional Software	12
Configuring the SNMP Agent	12
Configure Non-Default Ports or Passwords	12
Configuring Parameters	12
Configuring Virus Protection	13
Configuring Backup Software	13
Starting the SynapSense System	15
Upgrading or Modifying the Installation	17

Overview

SynapSense® Wireless Monitoring and Cooling Control is designed to help you visualize and better understand the environmental conditions inside of the data center. These tools can enable consistent, sustained measurement to enable short and longer-term energy savings and efficiencies.

Follow the instructions in this document to prepare for, install, and configure your SynapSense solution.

Panduit Technical Support

Severity 1 & 2 Issues:

Americas: 1-866-721-5302 x86810 during normal Central Standard Time business hours

EMEA: 44-1291-674-661 x22761 during normal U.K. business hours

APAC: 65-8200-3931 or 65-8200-3932 between 8 a.m. and 5 p.m. local time

Severity 3 & 4 Issues, Email - normal business hours:

systemsupport@panduit.com

Minimum System Requirements

The following minimum specifications must be met prior to installing the server components.

The standard configuration installs all components on a single server. If using a multiple server configuration, please consult with your Panduit Professional Services representative before proceeding.

If you are also installing SynapSense Active Control, see the Active Control Installation Guide for system requirements and installation instructions.

Server Hardware

- **Processor** – Quad-core Intel® Xeon® L5606 (2.10 GHz) or better
- **Memory** – 8 GB RAM (fully buffered) for core components. Add 1 GB of RAM for each additional optional component installed. Large installations may require 16 GB RAM and 2 GB of RAM for each optional component.
- **Disk Space** – 1 TB (hot-swap RAID recommended)
- **Connectivity** – 1 GB Ethernet adapters
- **Server Mode** – Operating system must be configured NOT to reboot automatically after receiving OS updates. Any automatic reboots should be disabled.¹ Incorrect termination of the SynapSense database could cause database corruption.

Server Software

- **Operating System** – Microsoft® Windows Server 2008 R2, 2012, or 2016. MapSense also runs on Windows® 10.
- **User Privileges** – Software installation requires the active user to have full administrator privileges.

Client PC

- **Supported Browsers** – Windows® Internet Explorer 11.x or higher, Mozilla® Firefox® 48.x or higher, and Google Chrome™ 55 or higher.
- **Flash Plug-in** – Adobe® Flash Player 11 or higher
- **Screen Resolution** – For the best display, a minimum resolution of 1280x1024 on Client PC display screens is recommended.

¹Manually restart the SynapSense Environment Server after an operating system update to verify that all services start with the new components. The SynapSense wireless network does not function if the server is restarted and the SynapSense Device Manager service does not start. This causes the wireless nodes to go into Sleep mode after several hours and can then take up to 24 hours to begin reporting again.

Preparing for Installation

Before installing the SynapSense software components, complete the following steps.

Static IP Address Allocation

A separate static IP address is required for the following:

- The SynapSense Environment Server
- Each SynapSense Gateway installed in the data center

Please ensure that these IP addresses are available prior to beginning the installation.

NOTE: If using the SynapSense Intelligent Gateway and DHCP, a static IP is not required for the Gateway.

Setup for SynapSense Gateways

SynapSense Gateways act as a communication bridge between the wireless network and the server located on an Ethernet network. Multiple Gateways are used for redundancy and wireless coverage.

In addition to the static IP address, each SynapSense Gateway requires:

- 110- or 240-volt power within three meters of its location
- An Ethernet connection with connectivity to the SynapSense server

See the *SynapSense Gateway Installation Guides* for details on how to set up SynapSense Gateways.

Setup for SynapSense Environment Server

Make sure to have these items configured prior to beginning the SynapSense installation process.

Configure TCP and UDP Ports

The tables below identify the TCP and UDP ports used by SynapSense applications. These ports should be made available through the SynapSense server firewall and any network routers.

Table 1 – Default Ports Used for External Communication

Application	Default Port Number	Comments
Gateway-Device Manager	10001	Port is used by Device Manager to communicate to SynapSense Gateways
SynapSense Web Console	8080	HTTP access to SynapSense Web Console. Port is configurable to any other unused port on the server.
SynapSense Web Console	8443	(Optional) HTTPS access to SynapSense Web Console. Port 8443 is used as the default port for SSL communication with the Web Console. This port is configurable.
SynapSense Livelmaging™	9091	HTTP access to SynapSense Livelmaging server.
GW Management	80	Browser interface to manage the SynapSense Gateway.
Alert notifications via e-mail (SMTP)	25	Email alerts (optional)
SNMP Traps	162	SNMP Service (optional)
SNMP Agent	161	SNMP Service (optional)
BACnet Gateway	47808	BACnet Module (optional)
Modbus/TCP (Gateway/Plugin)	502	Modbus Module (optional)
Jboss	4447	Used for ES/MapSense communication.

Table 2 – Default Ports Used for Internal Communication

Application	Default Port Number	Comments
SynapSense Database	3306	SynapSense database connection
SynapSense Web Console	8080	HTTP access to SynapSense Web Console. This port is configurable by the customer.
SynapSense Web Console	8443	(Optional) HTTPS access to SynapSense Web Console. This default port is configurable by the customer.
SynapSense Livelmaging™	9091	HTTP access to SynapSense Livelmaging server.

Application	Default Port Number	Comments
JBoss®	3783	JBoss application in the SynapSense server.
Jboss	4447	Used for ES/MapSense communication.
JBoss JNP	1099	JBoss Java Naming Protocol
JBoss JNP	1098	JBoss Java Naming Protocol
Device Manager RMI	2000	Device Manager Service
SNMP Agent Notification	1620	SNMP Service (optional)
BACnet Gateway RMI	1100	BACnet service (optional)

Disable Anti-Virus Software

Because of the extensive nature of the SynapSense system, you must disable any anti-virus software running on the server for the duration of the installation process.

Disable Admin Approval Mode

During installation, windows can show repeated messages asking for administrator approval before you can continue. The following steps disable that feature. Enable the feature again after the installation.

To disable Admin Approval Mode:

1. On the **Start** menu, click **All Programs > Accessories > Run**.
2. Type **secpol.msc** in the Run field, then click **OK**.
3. In the Local Security Settings window, select **Local Policies**.
4. Double-click **Security Options**.
5. Scroll to and double-click to open **User Account Control: Run all administrators in Admin Approval Mode**.
6. Click the **Disable** radio button, then click **OK**.
7. Restart the PC, if requested.
8. Close the **Local Security Settings** window.

Refer to the Microsoft website for more information about this feature and its uses.

SynapSense Installation

The SynapSense Setup wizard installs all the core and optional components selected. Please consult with your Panduit Professional Services representative to ensure the selection of appropriate components.

The standard SynapSense installation includes the following components:

- Environment Server
- Web Console
- MapSense
- Device Manager
- Livelmaging

Additional components available for installation include the following:

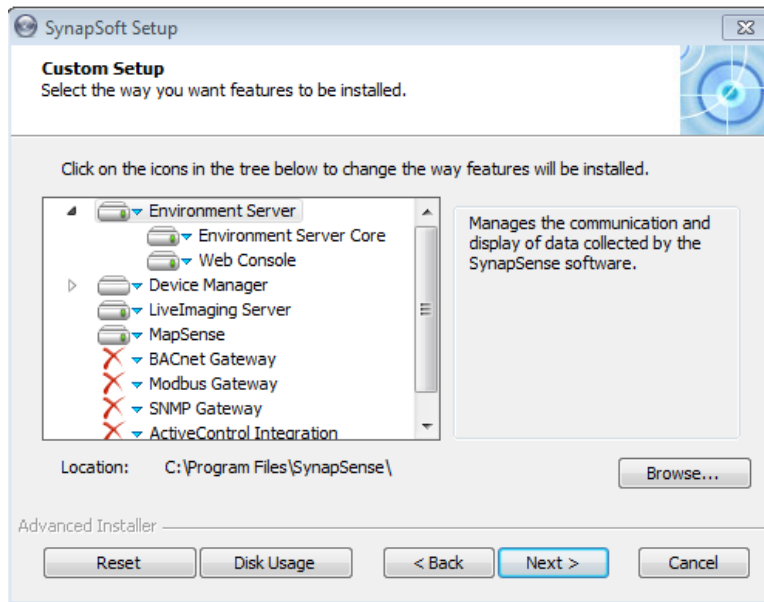
- Modbus Gateway
- SNMP Gateway
- BACnet Gateway

Note: See "Configure Optional Software" on page 12 for information about installing the optional components listed above.

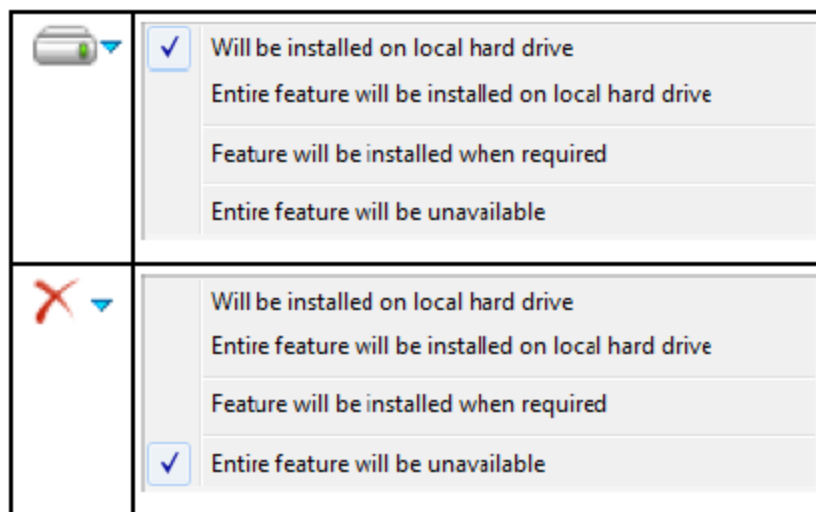
The procedure below guides you through the SynapSense installation process.

To install SynapSense software:

1. Insert the SynapSense Installation CD.
2. Select **SynapSense Setup.exe**.
3. When the Welcome window displays, click **Next**.
4. On the End-User License Agreement window, accept the agreement, and then click **Next**.
5. On the Custom Setup window, the core components are selected by default. Click **Next** to install *just* the core components.



6. To include additional components, do the following:
 - a. Scroll to the component you want to modify.
 - b. Select the blue arrow adjacent to the component name and select from the menu that displays. Components to be included in the install display a CPU icon, components excluded display an **X**.




- c. Click Next.
7. On the Database Configuration window, do the following:
 - a. Enter the root user password for the database or use the system default (**dbuser**).
 - b. Verify the default data location or click **Browse** to navigate to a different location

- on your network to store the data files.
- c. Click **Next**.
- 8. On the Ready to Install window, click **Install**.
- 9. Click **Finish** when the Completing the SynapSense Data Center Optimization Platform Setup Wizard displays.

Installing MapSense Separately

You can install the MapSense application on a machine that is separate from the Environment Server. See also: Opening an Existing Project in the *MapSense User Guide*.

To install a separate instance of MapSense:

1. Follow **Steps 1 through 4** of the Standard Installation.
2. On the Choose Setup Type window, click **Custom**.
3. On the Custom Setup window, do the following:
 - a. Ensure that MapSense has the included icon displayed.  If the icon is not present, select the blue arrow to display a menu, then select **Will be installed on the local hard drive**.
 - b. Ensure that every item on the list that is not MapSense has the excluded icon.  If the icon is not present, select the blue arrow to display the menu, then select **Entire feature will be unavailable**.
4. Click **Next**.
5. Continue with **Steps 6 through 8** of the Standard Installation procedure to complete the installation.

Configure Optional Software

If you are using third party programs for virus protection or backup software, there are additional configuration steps to complete. The following sections provide guidelines to consider when implementing these types of third-party applications.

Configuring the SNMP Agent

The SNMP Agent gives other systems a bridge into the SynapSense application. It is responsible for responding to SNMP queries for management information. The SNMP Agent uses an internal MIB (Management Information Base) file for hierarchical representation of available data. Data is provided to the management station in response to SNMP **get**, **get-next**, or **get-bulk** requests.

Configure Non-Default Ports or Passwords

In most cases, the default configuration is used and no further configuration is required. However, if the SynapSense Environment Server uses values for ports or private/public passwords, complete the following configurations steps:

1. Navigate to **C: Program Files >SynapSense >SynapSNMP >conf >SNMPConf.xml**.
2. Edit the SNMP Agent configuration file, **SNMPConf.xml**. If any configuration changes are made, the SynapSense SNMP Agent service must be restarted for the new configuration to take effect.

Configuring Parameters

The parameters to configure are as follows:

- **Network Interface** – This section should be changed if the server has more than one network interface card and SNMP traffic should only go out over one card. The default protocol is UDP, but can be changed to match your network management system.
- **v2c** – The **v2c enabled** tag is set to **true** by default. If your NMS only uses version 3 of the SNMP protocol, set **v2c enabled** to **false** and **v3 enabled** to **true**. You can also set the public and private community strings.

Note: **v2c enabled** and **v3 enabled** should never be set so both are either **true** or **false** at the same time.

- **v3** – If the NMS uses only SNMP version 3 to communicate, then set the v3 **enabled** tag to **true** (and set v2c **enabled** to **false**). You can then set up authentication and privacy as necessary. These settings must match your NMS settings.

Note: v2c **enabled** and v3 **enabled** should never be set so both are either **true** or **false** at the same time.

- **NotificationTargets** – This section can be duplicated for each SNMP trap target that must be configured. The only traps that are sent by the SynapSense SNMP Agent are startup and shutdown events. If your NMS does not need to process these traps, then this section should not be modified.
- **AgentXProtocol** – The **enabled** tag should be kept at the default value of **false**. If multiple AgentX SNMP Agents are installed and used on a single server, then contact your SynapSense Representative for assistance setting up the SynapSense SNMP service as a subagent of another.

Configuring Virus Protection

Configure any virus-scanning programs to ignore the SynapSense database data directory (for example, C:\Program Files\SynapSense\SynapSense DB\data). All the files in the directories under the data directory are binary data files and are not executed at any time.

Configuring Backup Software

Configure backup software to ignore the SynapSense database data directory (for example, C:\Program Files\SynapSense\SynapSense DB\data). The proper way to back up the database is to issue this command from the command line:

```
mysqldump -uroot -p<password> -e -q --single-transaction --  
events --routines synap > dbbackup.sql
```

This will back up all SynapSense data, plus any associated events.

NOTE: Replace the string <password> in the command line above with the password entered for the root user during installation.

This command creates a SQL script in the dbbackup.sql file that recreates the SynapSense database. The script file can be directed to another directory for automatic backup. With large databases (18 months of recording 10,000 sensors), this could take longer than an hour to complete.

It is important to back up the MapSense project file at the same time as the database. The MapSense project file must match with the database or an out of sync condition occurs and further updates to the system are not possible.

Starting the SynapSense System

Once you have installed all the software, started the services, and performed the necessary system configurations (if you are using virus or backup software), then you can start the SynapSense System.

To start the system:

1. Ensure that all of the following SynapSense services are running on the database server:

SynapSense Database
 SynapSense Device Manager
 SynapSense Environment Server
 SynapSense LivImaging Server

2. Ensure that any optional services are installed (for example, Modbus Gateway, BACnet Gateway, or SNMP Agent) by viewing their status in Windows Services. See the image below.

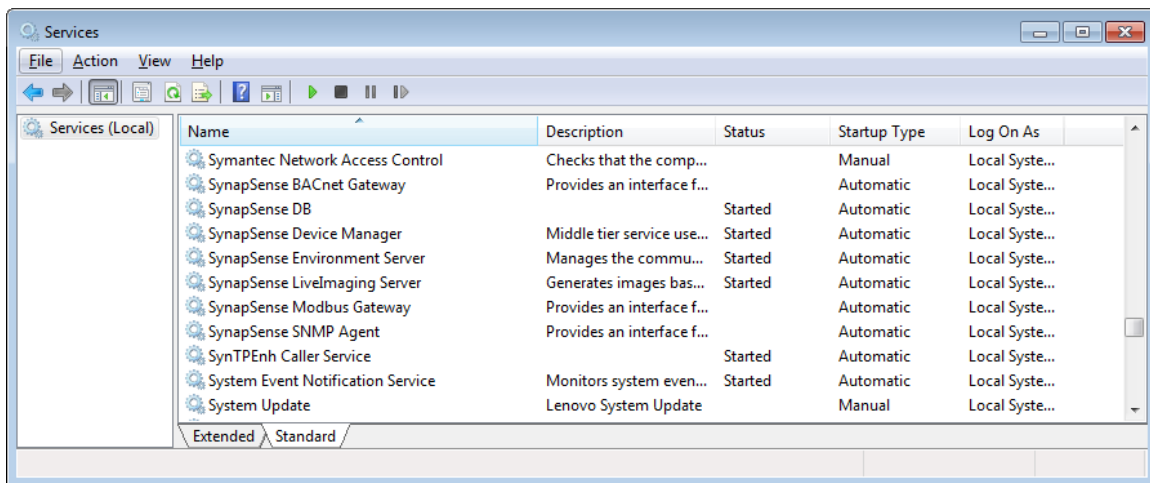


Figure 1 - Check that all services are running

3. Activate the wireless network. Do this by connecting the SynapSense Gateways to the same network to which the server machine is connected. Plug in any supporting hardware, and ensure that the nodes have all been turned ON.
4. Export the project file from the MapSense.

Note: Work with your Panduit Representative to obtain the

correct project file. See also the *MapSense User Manual*.

5. Launch the Web Console from the server or a client PC. To do this, click the newly-created desktop icon or select **SynapSense Web Console** from the SynapSense folder in the Start menu. Or, access the Web Console from a client by browsing to **http://<hostname>:8080/synapsoft** where hostname is the name of the SynapSense Environment server.
6. Ensure that the nodes have joined the network and are sending data. See the *Web Console User Manual* for details on using the SynapSense Web Console interface. Nodes can take up to one hour to join and begin sending data after being powered on.

Upgrading or Modifying the Installation

Panduit Customer Support creates a Technical Note for each new release to ensure a smooth transition for existing customers who wish to upgrade. Please contact your Panduit representative or Panduit Customer Support for information about an upgrade.