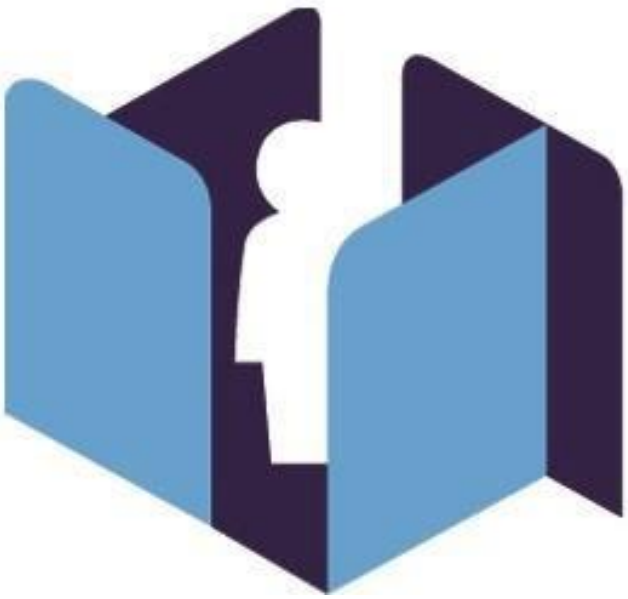


CHECKLIST FOR IT AND SECURITY PERSONNEL

PremiSys® v4.8

ABSTRACT

This document describes basic requirements for PC,Operating Systems and Networks for PremiSys Software

April 17, 2018

Updated May 8, 2023

Revision History

Revision Date	Revised By	Comments
6/5/2017	NSM	• Updated for PremiSys v2.22
6/12/2017	NSM	• Added more details for IP addressing of hardware devices • Added note regarding virtual environments • Added note regarding operating system security • Updated diagram to indicate specific type of communications used to communicate with ENGAGE Devices • Added section to describe Internet Access and moved note about licensing to this section
1/5/2018	NSM	• Updated for PremiSys v3.1
1/8/2018	NSM	• Updated PC Requirements
3/20/2018	NSM	• Corrected port requirements for Dashboard feature
4/17/2018	NSM	• Updated for PremiSys v3.2 • Eliminated outdated info pertaining to Windows XP support
5/8/2023	LGL	• Updated for PremiSys v4.8 • Updated PC Requirements • Changed references to PDC, IDenticard, or PDC IDenticard to PremiSys • Updated Operating System Requirements • Revised statement for installing software via download with optional DVD available for purchase. • Changed “IDenticard Windows Service” to “PremiSys Windows Service.” • Updated Database Requirements

Contents

Foreword

NOTE: “PremiSys” is used throughout these specifications to refer to both PremiSys and PremiSys Pro. “PremiSys and PremiSys Pro” or instances of one or the other are used when differentiation is needed.

Computer Requirements

Recommended Server

- Intel i5 Processor
  (4 cores) or equivalent
- 8+ GB RAM
- 1 GB free space on the hard drive for the PremiSys software (plus space for data)
- DVD drive
- Windows® Media Player or Desktop Experience, if playing sound files as audible alarms
- If you are installing a client with a server, such as in a "Full" installation, the following are also required:
  - Microsoft® Internet Explorer® 9 or later version
  - 1024 x 768 24-bit Video Card
  - USB ports for camera, printer, or other hardware

Client

- Intel i5 Processor
  (2 cores) or equivalent
- 4 GB RAM
- 650 MB free space on the hard drive for the PremiSys software (plus space for data)
- 1024 x 768 24-bit Video Card
- DVD drive, if installing from DVD media
- Microsoft® Internet Explorer® 9 or later version
- USB ports for camera, printer, or other hardware, if playing sound files as audible alarms

IMPORTANT

The specifications below are based largely on requirements for the Windows and the .NET Framework and subjective experience using PremiSys in various environments. You (or your PremiSys partner) should evaluate the needs of your specific system and determine the appropriate specifications for server and/or client computers based on current operating system requirements and the needs of your system.

Operating System Requirements

Supported Operating Systems

- Microsoft® Windows® Server 2019
- Microsoft® Windows® Server® 2016
- Microsoft® Windows® Server® 2012
- Microsoft® Windows® 10 (build 19042 or greater)
- Microsoft® Windows® 11

Notes

- See Installation Requirements for background on flexible installation options that affect OS requirements.
- Some client features of PremiSys include playing sounds which may not be supported on server operating systems.
- All operating systems for server(s) and clients should be properly secured and kept current with appropriate security updates from Microsoft.
- PremiSys components can be installed on suitable virtual environments. These virtual environments should meet or exceed the appropriate requirements from the section “Computer Requirements” above.

Network Requirements

Host Computer/ Server

- WARNING: Loss of network connectivity disables access-control functions designed to work across multiplecontrollers as well as other features. See the list of lost features at the end of this section.
- PremiSys controllers require a 10/100 Mb/s Ethernet network port, or alternatively, they can use RS-485 or RS-232 serial communications (see diagram at end of checklist).
- Communication between the PremiSys application server and each controller must be uninterruptible.
- The features listed below are lost when communication between the host computer and controllers is interrupted. Card reads, RTEs and their related operations (unlocking and point masking) still function. Transactions buffered in the controllers are uploaded to the host when communications are restored. Card changes are automatically downloaded when controllers come back online.
    - Photo recall
    - Configuring, monitoring and controlling all of the following, especially when single groups include items connected to more than one controller (includes monitoring and controlling via maps):
    - Doors and door groups
    - Elevators and elevator groups
    - Monitor points and monitor point groups
    - Alarms and alarm point groups
    - Control points and control point groups
    - Triggers and procedures in which the triggering component and the component acted on are on different controllers (global triggers and procedures).
    - Triggers and procedures using video as the action resulting from the trigger
    - Alarm acknowledgements
    - Downloading and resetting controllers
    - Upgrading controller firmware
    - Saving and/or downloading cardholders
    - Generating cards after a block add or update
    - Configuring, monitoring and controlling individual controllers and boards
    - Running procedure actions directly from a client (without triggers)
    - Up-to-date transaction displays, reports and journals
    - Scheduled un/lock events

IP Addressing

Application Server

The PremiSys application server must have a static IP address and be available to all clients. Alternatively, DHCP reservations can be used to achieve the same effect as static IP addresses.

Controllers

Each controller connected via a network should be assigned an IP address when it is initially configured. This address can be statically assigned or assigned using a DHCP reservation. Controllers are specified in PremiSys by IP address and cannot be configured using a FQDN, therefore DHCP without reservations is not supported. The IP address is programmed via the controller's built-in web application which is secured via a combination of username/password anda DIP switch setting on the board.

PoE One-Door Reader Boards

PoE One-Door Reader Boards can be assigned an IP address using one of three methods:

- Statically assigned using supplied, separate software utility
- Standard DHCP
- Proprietary DHCP (this protocol can coexist on the same network with a standard DHCP without adversely affecting other DHCP devices on the network).

ENGAGE Gateways

Each gateway device requires an IP address which can either be statically assigned or assigned by DHCP. The method is configured during the gateway setup process using the ENGAGE mobile application.

ENGAGE Locks

Each NDE or LE lock operating in Wi-Fi/Offline mode requires an IP address. The IP address can be either staticallyassigned or assigned by DHCP. The method is configured during the lock setup process using the ENGAGE mobileapplication.

Installation Requirements

General Requirements

- As required by Windows®, PremiSys must be installed by a logged-in Windows® user with full administrator rights.
- Software is available via download. Optionally, a DVD may be purchased and used for installation.

Flexible Installation Options

PremiSys offers flexible installation options whereby:

- The client and server software and all services can be installed on a single server (“Full” installation).
- The PremiSys Application Service can be installed singly on a dedicated server (“PremiSys Windows Service” installation).
- The Database can be installed separately on a dedicated database server (“Database” installation).
- Components that PremiSys uses to work with computers’ Windows® Internet Information Services can be installed separately on an IIS server (“Components Requiring IIS” installation).
- Clients can be installed on separate computers pointing to a dedicated PremiSys server (“Client” installation).

IIS Components

- PremiSys Pro and PremiSys require IIS. IIS can be installed on the PremiSys application server or a standalone IIS server. The IIS version is dependent on the OS version used. If it is an IIS version running on a supported OS, it is compatible.

Internet Access

Licensing Procedures

Internet access at the PremiSys application server is strongly suggested in order to allow licensing the software over the Internet. If Internet access is not possible, a phone call to PremiSys Technical Support can be made to manually complete licensing.

ENGAGE Site Creation

During the creation of the ENGAGE site within PremiSys software, which must be done from the PremiSys application server, the application server will need to contact the ENGAGE partner portal site.

ENGAGE Gateways and Locks

Each ENGAGE lock must be commissioned. This process requires the ENGAGE mobile app on a compatible device. During this process the lock communicates with the mobile device using Bluetooth, but the mobile device will require internet access in order to communicate with the ENGAGE partner portal.

Database Requirements

- PremiSys supports Microsoft® SQL Server 2012, 2014, 2016 and 2019. TLS-1.0 must be enabled.
- The PremiSys installation includes Microsoft® SQL Server® 2014 Express R2 if a SQL server is not already available. Microsoft defines the operating characteristics of this installed database and any limitations it may have. Neither Matrix Systems nor PremiSys has control over the specifications of this product.
- Two databases, Cardholders and PremiSys, attach to the database engine during installation.
- Administrative access in SQL, e.g., an “sa” login, is necessary to install or upgrade PremiSys or PremiSys Pro.
- The SQL server must support mixed mode authentication.
- PremiSys clients use a SQL login that is created during installation so they can connect to the database.
- PremiSys incorporates a module allowing backups of the system database. Users can select whether to include access-control transactions and/or cardholder photo and signature files in the backups.
- PremiSys also incorporates a module allowing the archiving of access-control transactions to maintain efficient database and controller-buffer functioning.
- SQL-level backups are always recommended and can be managed using SQL Server tools.

Ports Used

- WARNING: PremiSys sets exceptions only for Windows® firewalls on the application and/or IIS server. Any other firewalls must be handled separately.
- The ports listed below must be open for PremiSys to function over a network. These ports must not be blocked by routers, switches, or firewalls.
- Additional ports may be required for use by third-party systems working in conjunction with PremiSys. PremiSys has no control over, and cannot predict, these additional port requirements.
- A Windows® firewall exception is made for UDP Port 137, which is used for file share functions.
- A Windows® firewall exception is made for sqlbrowser.exe, which is used for interactions between the server and the database and the client and the database. Our use of sqlbrowser.exe is in keeping with the specifications Microsoft describes in its MSDN article "Using SQL Server Browser."

Network Ports

TCP Port	Origination	Destination	Details
80	Client	PremiSys IIS components	Photo recall, a feature whereby cardholder photos and other cardholder information are displayed when cards are presented.
443	Mobile Client	PremiSys IIS components	Mobile application
3001	PoE One-Door ReaderBoard	IP Controller 2-Reader Controller PoE 1-Door Reader Controller	Each Board acts as a TCP server listening on port 3001. The port is not user-configurable. The Controller connects as a TCP client to each Board. Each Board supports one and only one EP connection.
6005	PremiSys ApplicationServer	Mercury® Hardware	Default TCP Port used to communicate with controllers. NOTE: If this port is not available, it can be changed in thePremiSys software (Controller Configuration).
9000	Client	PremiSys Application Server	Used by the PremiSys Application Service, which interfaces with clients, the database and the access control hardware.
9002	Client	PremiSys Application Server	Used by the APIService.†
			Used by FileCache, which is an internal file share service. PremiSysuses FileCache to handle internal files, such as the sound files for alarm acknowledgement or the files created when running the internal transaction archiving module in PremiSys.
			Used by PremiSysInternalService, which is an internal communication server between a PremiSys client and the PhotoRecall web service.
			Used by QueryAPIService,† which provides API support.
			Used by StatusAPIService,† which provides API support for access control hardware status.
			Used by ActionAPIService,† which provides API support for access control actions on hardware.
			Used by AlarmAckAPIService,† which provides API support forAlarm Acknowledgement.
9003	Client	PremiSys IIS components	Used by PremiSysWcfService, which is an internal communication service between a PremiSys client and the Photo Recall Web service; it is also used for the Cardholder API. The Photo Recall Web service is behind IIS.
	Client (or Web Browser)	PremiSys Application Server	Dashboard
80/443	Engage® NDE Lock	PremiSys IIS Components	Used by Engage® NDE-Series locks in WiFi Mode. Port 80 is used ifthe locks are in unsecure mode, otherwise port 443 is used.
443	PremiSys ApplicationServer	Engage® Gateway	Used by Engage® Gateway in IP Mode.

† This service is only enabled when licensed after purchase of an add-on module.

NOTE: The table above describes port usage for new PremiSys installations. Upgraded systems may be configured using specifications for the original version of PremiSys.

Diagrams

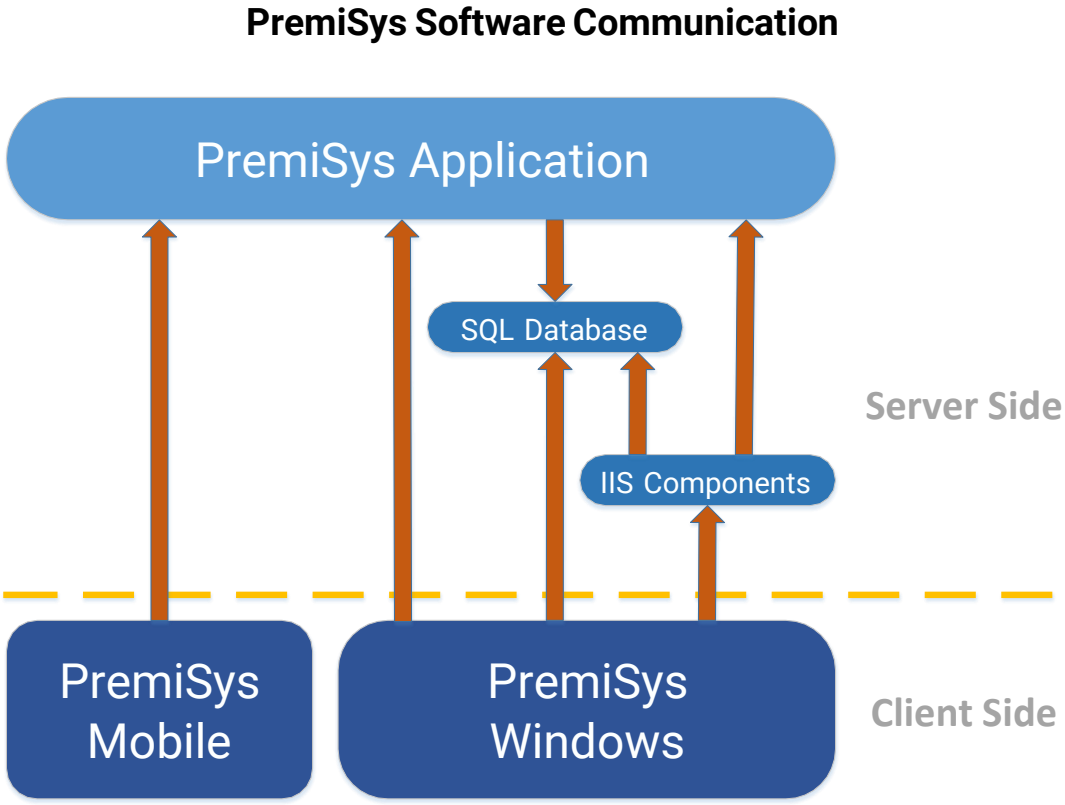


Figure 1 - Software components and communication

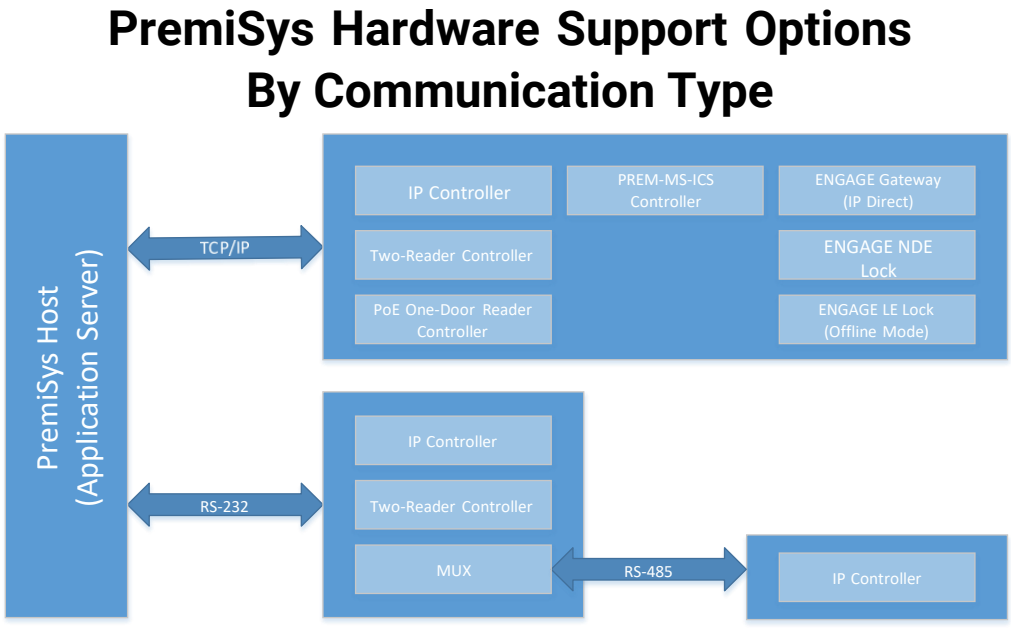
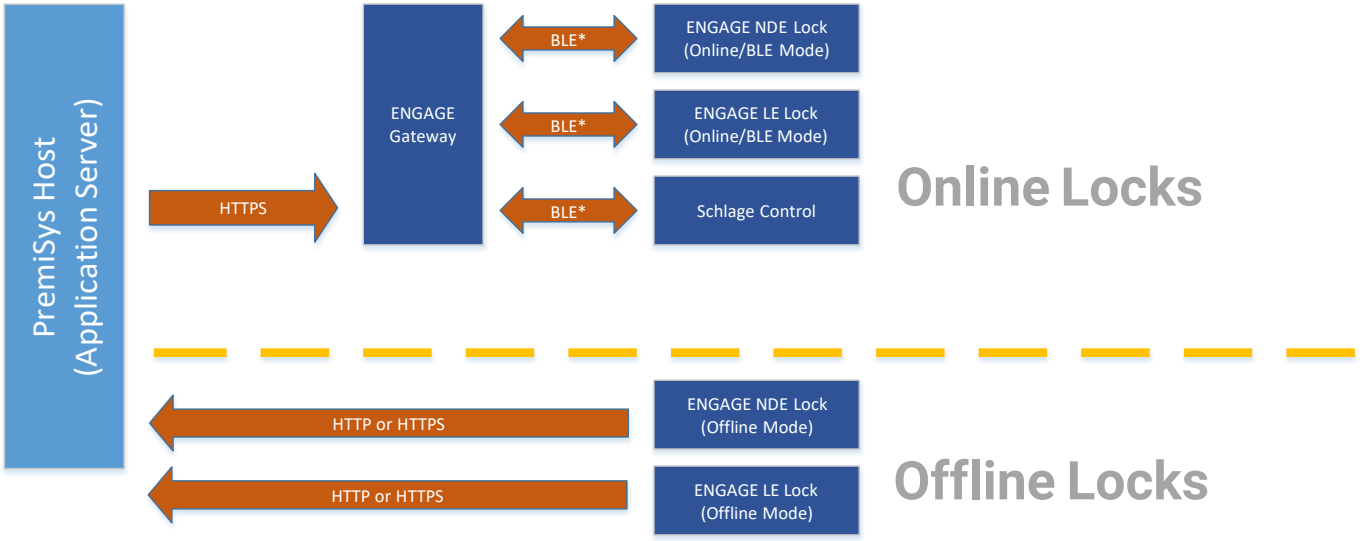


Figure 2 – Hardware support options by communication type

PremiSys ENGAGE Communication Options



* BLE Communications is encrypted using AES-256-CBC

Figure 3 – ENGAGE Communication Options