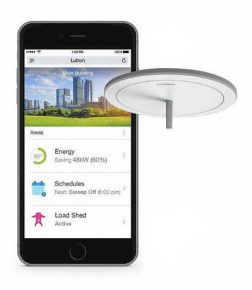


LUTRON Vive Vue Total Light Management System User Guide

Vive Vue
Total Light Management System
IT Implementation Guide

Revision C 19 January 2021

Contents

Vive Security Statement

Lutron takes the security of the Vive Lighting Control System very seriously
The Vive Lighting Control System has been designed and engineered with attention to security since its inception Lutron has engaged security experts and independent testing firms throughout the entire development of the Vive Lighting Control System Lutron is committed to the security and continuous improvement throughout the Vive product lifecycle
The Vive Lighting Control System uses a multi-tiered approach to security and National Institute of Standards and Technology (NIST)-recommended techniques for security
They include:

1. An architecture that isolates the wired Ethernet network from the wireless network, which strictly limits the possibility of the Vive Wi-Fi being used to access the corporate network and gain confidential information
2. A distributed security architecture with each hub having its own unique keys that would limit any potential breach to only a small area of the system
3. Multiple levels of password protection (Wi-Fi network and the hubs themselves), with built-in rules that force the user to enter a strong password
4. NIST-recommended best practices including salting and SCrypt for securely storing usernames and passwords
5. AES 128-bit encryption for network communications
6. HTTPS (TLS 1 2) protocol for securing connections to the hub over the wired network
7. WPA2 technology for securing connections to the hub over the Wi-Fi network

8. Azure provided encryption-at-rest technologies

The Vive hub can be deployed in one of two ways:

- Dedicated Lutron Network
- Connected to the corporate IT network via an Ethernet connection The Vive hub must be connected via Ethernet when connected to the Vive Vue Server as well as to access certain features such as BACnet for BMS integration Lutron advises following best practices in this instance, including separating the business information network and the building infrastructure network Use of a VLAN or physically separated networks is recommended for secure deployment

Corporate IT Network Deployment
The Vive hub must be deployed with a fixed IP Once the IT network is operational, the Vive hub will serve password-protected web pages for access and maintenance The Vive hub Wi-Fi may be disabled if desired The Vive hub Wi-Fi is NOT required when connecting the Vive hub to the Vive
Vue server
The Vive hub acts as a Wi-Fi access point purely for the configuration and commissioning of the Vive system It is not a substitute for your building's normal Wi-Fi access point The Vive hub does not act as a bridge between wireless and wired networks It is strongly recommended that local IT security professionals be involved with the network configuration and set-up to ensure the installation meets their security needs

Network and IT Considerations

Network Architecture Overview

What is on the traditional network IP architecture? – The Vive Hub, Vive Vue server, and client devices (eg PC, laptop, tablet, etc)
What is NOT on the traditional network IP architecture? – The lighting actuators, sensors, and load controllers are not on the network architecture This includes Pico wireless controls, occupancy and daylight sensors, and load controllers These devices communicate on a Lutron proprietary wireless communication network

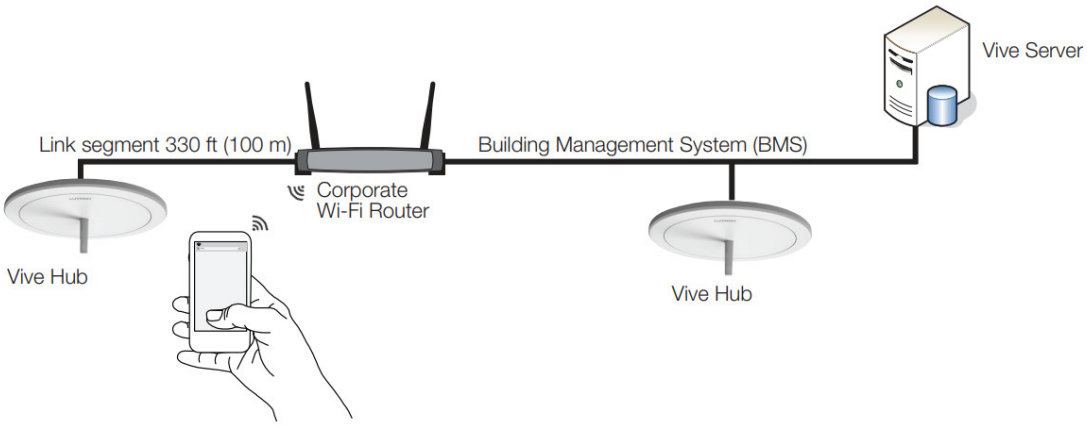
Physical Medium

IEEE 802.3 Ethernet – Is the physical medium standard for the network between Vive hubs and the Vive server Each Vive hub has a female RJ45 connector for a LAN connection CAT5e – The minimum network wire specification of the Vive LAN/VLAN

IP Addressing

IPv4 – The addressing scheme used for the Vive system The IPv4 address should be static but a DHCP reservation system can also be used Standard DHCP lease is not allowed DNS Hostname is not supported The IPv4 address can be field-set to any range, Class A, B, or C Static will be assumed

Network and IT Considerations (continued)
Corporate Network



Ports Used – Vive Hub

Traffic	Port	Type	Connection	Description
Outbound	47808	UDP	Ethernet	Used for BACnet integration into Building Management Systems
	80	TCP		Used to discover the Vive Hub when mDNS is not avail able
	5353	UDP	Ethernet	Used to discover the Vive Hub via mDNS
Inbound	443	TCP	Both Wi-Fi and Ethernet	Used to access the Vive hub webpage
	80	TCP	Both Wi-Fi and Ethernet	Used to access the Vive hub webpage and when DNS i s not available
	8081	TCP	Ethernet	Used to communicate with the Vive Vue server
	8083	TCP	Ethernet	Used to communicate with the Vive Vue server
	8444	TCP	Ethernet	Used to communicate with the Vive Vue server
	47808	UPD	Ethernet	Used for BACnet integration into Building Management Systems
	5353	UDP	Ethernet	Used to discover the Vive Hub via mDNS

Ports Used – Vive Vue Server

Traffic	Port	Type	Description
Inbound	80	TCP	Used to access the Vive Vue webpage
	443	TCP	Used to access the Vive Vue webpage
	5353	UDP	Used to discover the Vive Hub via mDNS
Outbound	80	TCP	Used to discover the Vive Hub when mDNS is not available
	8081	TCP	Used to communicate with the Vive Vue server
	8083	TCP	Used to communicate with the Vive Vue server
	8444	TCP	Used to communicate with the Vive Vue server
	5353	UDP	Used to discover the Vive Hub via mDNS

Network and IT Considerations (continued)

Protocols Required

ICMP – used to indicate that a host could not be reached mDNS – protocol resolves hostnames to IP addresses within small networks that do not include a local name server
BACnet/IP – BACnet is a communications protocol for building automation and control networks It is defined in ASHRAE/ANSI standard 135 Below are details on how the Vive system implements BACnet communications

- BACnet communication is used to allow two-way communication between the Vive system and a Building Management System (BMS) for control and monitoring of the system
- The Vive hubs adhere to Annex J of the BACnet standard Annex J defines BACnet/IP which uses BACnet communication over a TCP/IP network
- The BMS communicates directly to the Vive hubs; not to the Vive server
- If the BMS is on a different subnet than the Vive hubs then BACnet/IP Broadcast Management Devices (BBMDs) can be used to allow the BMS to communicate across subnets

Network and IT Considerations (continued)

TLS 1.2 Ciphers Suites

Required Ciphers Suites

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Ciphers Suites recommended to be disabled

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_NULL_SHA
- SSL_CK_RC4_128_WITH_MD5

- SSL_CK_DES_192_EDE3_CBC_WITH_MD5
- TLS_RSA_WITH_RC4_128_MD5

Communication Speed and Bandwidth

100 BaseT – Is the fundamental communication speed for the Vive hub and Vive Vue server communications

Latency

Vive hub to Vive server (both directions) must be <100 ms

Wi-Fi

Note: The Vive hub is equipped with Wi-Fi (IEEE 802 11) enabled by default for ease of setup, The Wi-Fi on the Vive hub can be disabled if required as long the Vive hub is connected and accessible via the wired Ethernet network

Server and Application Considerations

windows OS Requirements

Software Version	Microsoft® SQL Version	Microsoft® OS Version
Vive Vue 1.7.47 and older	SQL 2012 Express (default) SQL 2012 Full (requires custom installation)	Windows® 2016 Server (64-bit) Windows® 2019 Server (64-bit)
Vive Vue 1.7.49 and newer	SQL 2019 Express (default) Full SQL 2019 (requires custom installation)	Windows® 2016 Server (64-bit) Windows® 2019 Server (64-bit)

Hardware Requirements

- Processor: Intel Xeon (4 cores, 8 threads 2 5 GHz) or AMD equivalent
- 16 GB RAM
- 500 GB hard drive
- Screen with minimum 1280 x 1024 resolution
- Two (2) 100 MB Ethernet network interfaces
  – One (1) Ethernet network interface will be used for communication to Vive wireless hubs
  – One (1) Ethernet network interface will be used for communication to corporate intranet, allowing access from Vive Vue

Note: Only one (1) Ethernet network interface is used if all Vive wireless hubs and client PCs are on the same network

Server and Application Considerations (continued)

Non-Dependent System Server

The lighting system can fully function without server connectivity Loss of server connectivity does not affect timeclock events, lighting overrides, BACnet, sensor control, or any other daily functionality The server services

two functions;

1. Enables Single End User UI – Provides the webserver for Vive Vue, display system status and control
2. Historical Data Collection – All energy management and asset management is stored on the SQL logging server for reporting

SQL Server Database Usage

Vive Composite Data Store Database – Stores all of the configuration information for the Vive Vue server (Vive Hubs, area mapping, hotspots) A locally installed instance of SQL Server Express edition is best suited for this database and is automatically installed and configured during installation of Vive Vue on the server Due to the operations performed (backup, restore, etc) the Vive Vue software requires high-level permissions to this database
Composite Reporting Database – Real-time database that stores energy consumption data for the lighting control system Used to show energy reports in Vive Vue Data is recorded at an area level every time there is a change in the system
Composite Elmah Database – Error reporting database to capture historical error reports for troubleshooting
Composite Vue Database – Cache database for Vive Vue to improve web server performance

Database Size

Typically, each database is capped at 10 GB when using SQL Server 2012 Express edition If this database is deployed to a customer-supplied instance of SQL Server full edition on the application server, the 10 GB limit need not apply and the policy for data retention can be specified using Vive Vue configuration options

SQL Instance Requirements

- Lutron requests a dedicated SQL instance for all installs for data integrity and reliability
- A Vive system does not support remote SQL The SQL instance must be installed on the application server
- System administrator privileges are required for the software to access the SQL instance

SQL Access

Lutron applications use “sa” user and “sysadmin” permission levels with SQL Server because the applications need backup, restore, create new, delete and modify permissions under normal use, The username and password can be changed but the privileges are required Note that only SQL authentication is supported

WindowsR Services

The Composite Lutron Service Manager is a WindowsR service that runs on the Vive Vue server and provides status information about key Vive applications and also ensures that they are running any time the machine is restarted The Composite Lutron Service Manager UI application coincides with the Composite Lutron Service Manager service which should always be running on the server machine It can be accessed using the small blue “gears” icon in the system tray or from Services within the WindowsR operating system

Active Directory (AD)

Individual user accounts in the Vive Vue server can be set up and identified using the AD During setup, each user account can be set up with a direct application individual name and password or with authentication using Integrated WindowsR Authentication (IWA) Active directory is not used for the application but for individual user accounts

IIS

IIS is required to be installed on the Application Server to host the Vive Vue web page The minimum version required is IIS 10 **A recommendation of installing all features listed for IIS is advised.**

Feature Name	Required	Comment
FTP Server		
FTP Extensibility	no	
FTP Service	no	
Web Management Tools		
IIS 6 Management Compatibility		
IIS 6 Management Console	no	Allows you to use existing IIS 6.0 APIs and script s to manage this IIS 10 and above web server.
IIS 6 Scripting Tools	no	Allows you to use existing IIS 6.0 APIs and script s to manage this IIS 10 and above web server.
IIS 6 WMI Compatibility	no	Allows you to use existing IIS 6.0 APIs and script s to manage this IIS 10 and above web server.
IIS Metabase and IIS 6 Configuration Compatibil ity	no	Allows you to use existing IIS 6.0 APIs and script s to manage this IIS 10 and above web server.
IIS Management Console	yes	Installs web server Management Console which supports management of local and remote web servers
IIS Management Scripts and tools	yes	Manages a local webserver with IIS configuratio n scripts.
IIS Management Services	yes	Allows this webserver to be managed remotely fr om another computer via the web server Manag ement Console.

World Wide Web Services		
Common HTTP Features		
Static Content	yes	Serves .htm, .html, and image files from a website.
Default Document	no	Allows you to specify a default file to be loaded when users do not specify a file in a request URL.
Directory Browsing	no	Allow clients to see the contents of a directory on your web server.
HTTP Errors	no	Installs HTTP Error files. Allows you to customize the error messages returned to clients.
WebDav Publishing	no	
HTTP Redirection	no	Provides support to redirect client requests to a specific destination
Application Development Features		
ASP.NET	yes	Enables webserver to host ASP.NET applications.
.NET Extensibility	yes	Enables webserver to host .NET framework-managed module extensions.
ASP	no	Enables webserver to host Classic ASP applications.
CGI	no	Enables support for CGI executables.
ISAPI Extensions	yes	Allows ISAPI extensions to handle client requests.
ISAPI Filters	yes	Allows ISAPI filters to modify web server behavior.
Server-Side Includes	no	Provides support for .stm, .shtm, and .shtml include files.

IIS Features (continued)

Feature Name	Required	Comment
Health and Diagnostics Features		
HTTP Logging	yes	Enables logging of website activity for this server.
Logging Tools	yes	Installs IIS logging tools and scripts.
Request Monitor	yes	Monitors server, site, and application health.
Tracing	yes	Enables tracing for ASP.NET applications and failed requests.
Custom Logging	yes	Enables support for custom logging for web servers, sites, and applications.
ODBC Logging	no	Enables support for logging to an ODBC-compliant database.
Security Features		
Basic Authentication	no	Requires a valid Windows* user name and password for connection.
Windows* Authentication	no	Authenticates clients by using NTLM or Kerberos..
Digest Authentication	no	Authenticates clients by sending a password hash to a Windows* domain controller.
Client Certificate Mapping Authentication	no	Authenticates client certificates with Active Directory accounts.
IIS Client Certificate Mapping Authentication	no	Maps client certificates 1 -to-1 or many-to-1 to a Windows. security identity.
URL Authorization	no	Authorizes client access to the URLs that comprise a web application.
Request Filtering	yes	Configures rules to block selected client requests.
IP and Domain Restrictions	no	Allows or denies content access based on IP address or domain name.
Performance Features		
Static Content Compression	no	Compresses static content before returning it to a client.
Dynamic Content Compression	no	Compresses dynamic content before returning it to a client.

Browser UI (Vive Vue)

The main UI into the Vive system for Vive Vue and is browser-based Below are the supported browsers for Vive

Vue

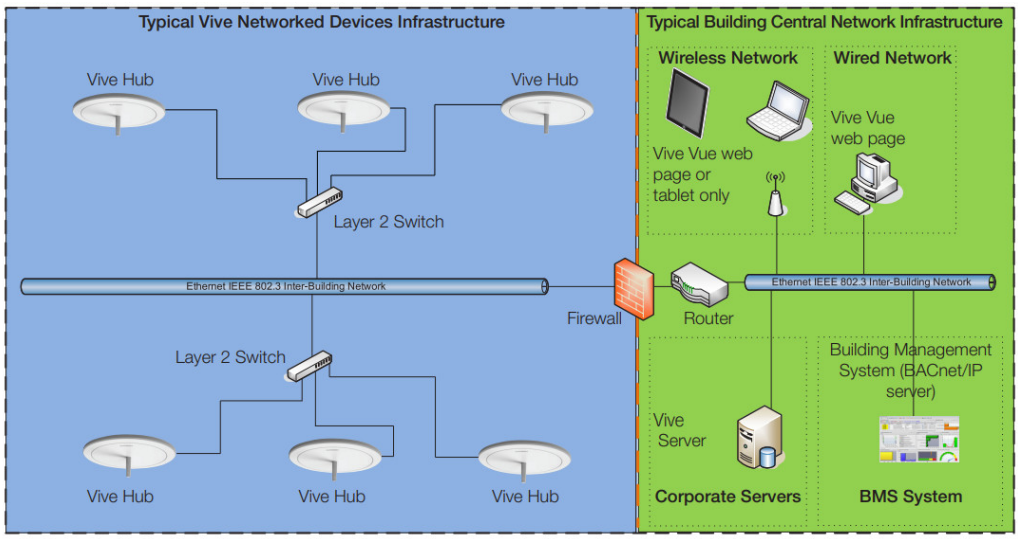
Browser Options

Device	Browser
iPad Air, iPad Mini 2+, or iPad Pro	Safari (iOS 10 or 11)
Windows laptop, desktop, or tablet	Google Chromes Version 49 or higher

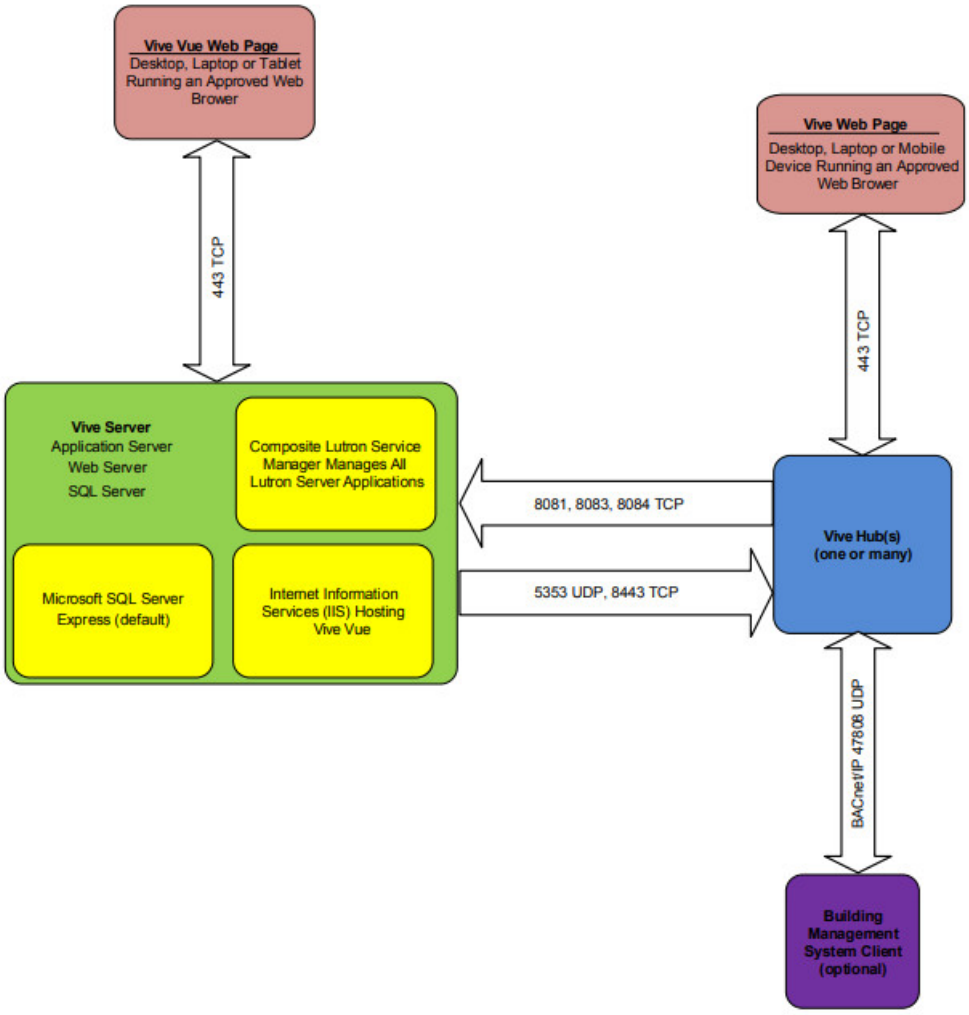
Software Maintenance

1. Each software is designed and tested to work on a specified Windows Operating System Versions See page 8 of this document for which versions of the Vive Vue software are compatible with each version of Windows and SQL
2. Lutron recommends keeping the Windows Servers that are used with a system up to date on all Windows patches that have been recommended by the customer's IT department
3. Lutron recommends installing, configuring, and updating an anti-virus program, such as Symantec, on any Server or PC running the Vive Vue software
4. Lutron recommends purchasing a Software Maintenance Agreement (SMA) offered by Lutron A software maintenance agreement gives you access to updated builds (patches) of a specific version of the software as well as access to new versions of Vive Vue software as they become available Patches are released to fix software defects identified and incompatibilities found with Windows updates New versions of Vive Vue software are released to add support for newer versions of Windows Operating Systems and versions of Microsoft SQL Server as well as to add new features to the product
5. Firmware updates for the Vive Hub can be found on www.lutron.com/vive Lutron recommends keeping the Vive Hub software up to date

Typical System Network Diagram



Communication Port Diagram



Customer Assistance

If you have questions concerning the installation or operation of this product, call the Lutron Customer Assistance
Please provide the exact model number when calling
The model number can be found on the product packaging
Example: SZ-CI-PRG
U S A , Canada, and the Caribbean: 1 844 LUTRON1
Other countries call: +1 610 282 3800
Fax: +1 610 282 1243
Visit us on the web at **www.lutron.com**

P/N 040437 Rev C 01/2021

LUTRON

Lutron Electronics Co, Inc
7200 Suter Road
Coopersburg, PA 18036 USA

Documents / Resources

	**LUTRON Vive Vue Total Light Management System** [pdf] User Guide LUTRON, Vive Vue, Total Light Management System