trellis™

The TRELLIS™ Real-Time Infrastructure Optimization Platform

Pre-Installation

Installer/User Guide

EMERSON™
Network Power

**For important safety information, visit:
www.emersonnetworkpower.com/ComplianceRegulatoryInfo**

This document supports versions up to 4.0.3 and higher.

TABLE OF CONTENTS

Preparing for the Installation

The *Trellis*™ Real-Time Infrastructure Optimization Platform installation process is performed by our Professional Services team members. However, there are some activities that need to be performed by our customers before our team arrives. We have created this guide to help you prepare for our arrival and to ensure a successful *Trellis*™ platform installation.

This guide includes the minimum hardware and software requirements, instructions to install the operating system, special tools to be used during the installation and information that you need to provide to our team in advance of our arrival. General information includes network communication, environments and installation scenarios.

NOTE: In this guide, the word platform refers to the *Trellis*™ platform and the word appliance refers to the Avocent® Universal Management Gateway appliance unless stated otherwise.

For additional information, please see the following guides:

The TRELLIS™ Real-Time Infrastructure Optimization Platform User Guide

The TRELLIS™ Real-Time Infrastructure Optimization Platform Linux® Red Hat® and Ubuntu Administrator's Guide

The TRELLIS™ Real-Time Infrastructure Optimization Platform Microsoft® Windows® Administrator's Guide

The TRELLIS™ Real-Time Infrastructure Optimization Platform Disaster Recovery Technical Bulletin

Avocent® Universal Management Gateway Appliance Installer/User Guide

Minimum Deployment Requirements

The minimum requirements for the deployment of the *Trellis*™ platform software include a customer-supplied Windows-based client workstation and two customer-supplied, dedicated server class machines, referred to as the front and back machines. The workstation and the front and back machines should be fully installed and equipped with the specified operating system, tools and provisioning requirements before the Professional Services team arrives to install the *Trellis*™ platform software.

The workstation is used by the Professional Services team to perform the software installation and the server class machines are used to house the *Trellis*™ platform. The front machine hosts the application servers and the back machine hosts the database servers and services, such as authentication. Both the front and back machines must be accessible from the workstation.

NOTE: The *Trellis*™ platform installers are delivered via the Content Delivery Network (CDN). Once downloaded, they must be extracted to the front and back machines or to a network share that is accessible from both machines.

NOTE: Make sure you are using a system that has the ability to share the installation configuration. For the following installation, an NFS/SMB system is used, which meets the sharing requirement.

NOTE: Avocent® supports the *Trellis*™ platform on physical and virtual server environments meeting the product documentation system specifications with dedicated system resources. While best performance is generally achieved in dedicated physical systems, virtual deployment can be effective as long as system resources are dedicated to the *Trellis*™ platform Virtual Machine (VM) instance. For virtually hosted environments, Avocent Technical Support will make every attempt to support any issues in the same manner that they would support the software in a physical server environment. Should an issue prove to be related exclusively to a virtually hosted environment, Avocent Technical Support will make all appropriate recommendations to the customer for optimal operations; assistance may be required by the corresponding Virtual Host Solution Provider to fully resolve those environmental related issues.

The following sections provide the minimum deployment requirements for the workstation, *Trellis*™ platform and the *Trellis*™ Intelligence Engine. See TRELLIS™ platform on page 3 for the machine and operating system requirements. See TRELLIS™ Intelligence Engine hardware requirements and pre-requisites on page 10 for the hardware and operating system requirements.

Workstation

The following are the minimum hardware and software requirements for the workstation to facilitate installation of the *Trellis*™ platform, version 4.0.3 and higher. These requirements are also applicable for the Bulk Data Processing tool. For more about the Bulk Data Processing tool, see Data Management in The TRELLIS™ Real-Time Infrastructure Optimization Platform User Guide.

NOTE: The workstation requirements are not applicable for the *Trellis*™ Express platform.

Hardware

- Dual-core Intel® Pentium® 4 CPU at 2.8 GHz
- 8 GB RAM, LAN connection

Operating systems

- Microsoft® Windows® 7
- Red Hat® Enterprise Linux® version 5.6 or higher

Additional software

- Adobe® Flash® Player version 12 or higher
- Notepad++
- Microsoft® RDP Client (if installing the *Trellis*™ platform on Windows®)
- PuTTY (if installing the *Trellis*™ platform on Linux® or configuring the Avocent® Universal Management Gateway appliance)
- WinSCP (if installing the *Trellis*™ platform on Linux®)

Browsers for the *Trellis*™ platform user interface

- Mozilla® Firefox® version 31.0 or higher
- Google Chrome™ version 40.0 to 54.0

- Microsoft Internet Explorer® 11

Browsers for the symbol portal

- Microsoft Internet Explorer® 11

Browsers for 3D features

- Microsoft Internet Explorer® 11, Chrome and Firefox

NOTE: The recommended minimum screen resolution is 1280 x 1024.

For more information, see Browser Recommendations on page 29.

TRELLIS™ platform

The following are the minimum deployment requirements for the *Trellis*™ platform, version 4.0.3 and higher.

Front and back machines

The following are minimum requirements on both the dedicated front and back machines to facilitate installation and operation of the *Trellis*™ platform.

NOTE: The front and back machine requirements are not applicable for the *Trellis*™ Express platform. Both the front and back machines must be dedicated to the *Trellis*™ platform.

Data Center Guidelines

Components	Small	Medium	Large	Enterprise
Concurrent users	10	20	50	100
Devices	2,000	20,000	100,000	200,000
Power Connections	1,000	10,000	60,000	100,000
Data Connections	2,000	10,000	60,000	100,000
Monitored Datapoints	1,000	10,000	40,000	140,000
CPUs	2	4	4	4
Cores	8	16	16	32

Hardware Recommendations

Front Machine	Small	Medium	Large	Enterprise
CPU manufacturer	Intel®	Intel®	Intel®	Intel®
CPU model	Xeon®	Xeon®	Xeon®	Xeon®
CPU speed (GHz) 8 M L3 cache	2.6	2.6	2.6	2.6
CPU count	1	2	2	2

CPU cores	4	4	4	8
Memory (GB) DDR3 1333 MHz	32	32	40	44
Disk throughput	> 500 MB/s (sequential) [uncached]			
Storage	300 GB Enterprise class			
Ethernet	> 80 MB/s			

Back Machine	Small	Medium	Large	Enterprise
CPU manufacturer	Intel®	Intel®	Intel®	Intel®
CPU model	Xeon®	Xeon®	Xeon®	Xeon®
CPU speed (GHz) 8 M L3 cache	2.6	2.6	2.6	2.6
CPU count	1	2	2	2
CPU cores	4	4	4	8
Memory (GB) DDR3 1333 MHz	24	32	32	32
Disk throughput	> 500 MB/s (sequential) [uncached]			
Storage	*300 GB Enterprise class for base installation			
Ethernet	> 80 MB/s			

*Hardware sizing varies depending on usage requirements and is performed by Professional Services.

Operating systems

The *Trellis*™ platform supports the following operating systems and software. One of the following operating systems must be installed on both the front and back machines:

- Microsoft® Windows® 2008, R2 SP1 Enterprise, 64-bit (full installation)
- Red Hat® Enterprise Linux® version 6.4, 6.5 or 6.6, 64-bit

NOTE: Local administrative rights and remote desktop access are required to perform the *Trellis*™ platform installation. Use only the true Administrator account when installing the *Trellis*™ platform software or patches, and for all occasions where the *Trellis*™ platform is shut down or restarted.

Windows OS

The full installation of the Windows operating system must be complete.

OS configuration

The configuration settings must be set up as follows.

Installation directories

The *Trellis*™ platform is installed to the C: drive by default. If you would like the platform installed to a different location, a symbolic link must be created to the following folders:

- c:\u01
- c:\u02

- c:\u03
- c:\u05

User configuration

All *Trellis*™ platform startups, shutdowns, installations, patches and upgrades must be performed using a Service Account with local Administrator privileges or by using the Administrator account.

NOTE: Always install, upgrade or patch the *Trellis*™ platform using the same Service Account.

NOTE: The front and back machine's operating system must have regional settings set to US English and the location set to United States.

Security configuration

The following are requirements for the configuration of security:

- Disable any Antivirus prior to the installation of the *Trellis*™ platform.
- Disable the Windows® Firewall on all three profiles (domain, private and public) prior to the installation of the *Trellis*™ platform.
- Disable the automatic Windows® updates.
- Always enable the UAC mode unless the installation is using the Administrator account.
- Restart the operating system after applying the UAC change.

VM requirements

The following VM platforms are supported when installing the *Trellis*™ platform in a virtual environment:

- Hyper-V 2012 R2 version 6.3 or higher (requires the Hyper-V Integration Services are installed on the guest operating system of the VMs that are housing the *Trellis*™ platform).
- VSphere version 4 or higher (requires all VMware tools are installed on the guest operating system of the VMs that are housing the *Trellis*™ platform).

Linux OS

The Linux operating system must be installed and provisioned for both the back and front machine using the supplied kickstart configuration file. The kickstart file ensures the operating system is ready for a successful *Trellis*™ platform installation.

You will receive the kickstart installation media from the Professional Services team before the scheduled date for OS provisioning or during the OS Requirements workshop.

Using kickstart

After obtaining the kickstart file, it must be customized to reflect the network topology of the environment. Specifically, the IP address and identity of the front and back machines must be modified, as well as the passwords for both the root and oracle users.

If a customer wishes to use their own kickstart configuration file, the Linux server administrator must incorporate all supplied kickstart file configuration settings into the operating system. Failure to do so could result in issues when running the *Trellis*™ platform installer.

CAUTION: Any changes to the supplied kickstart settings must be provided to the Professional Services team prior to installing the operating system, to allow time for assessment by the Engineering team. If any required configurations are absent, the installation may not be supported.

To locate and prepare the kickstart:

1. Copy the supplied *kickstart.cfg* file from the media to a location that can be reached by the front and back machines.
2. Open the *kickstart.cfg* file and edit the IP addresses, netmask, gateway and host filename for the machine on which the Linux operating system is to be installed. Then edit the root password and the oracle password.

CAUTION: Underscores are not supported in host filenames. The *Trellis*™ platform software requires a static IP. Changing the IP address after installation may render the software unusable.

To boot from the kickstart scripts to install the Linux libraries:

1. While booting at the virtual console of the back machine, press **F1**.
2. To make sure that distribution is supported, at the boot prompt enter **linux rescue_** to boot off a USB and load the available drivers. Using this technique, you can confirm the names of the hard drives (usually /dev/sda) and the name of the network device. If the devices are not supported, you may need to follow the instructions provided by Red Hat to get the latest drivers for your hardware and make sure the distribution supports the hardware. See http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Installation_Guide/s1-kickstart2-startinginstall.html for more information.
3. To verify the devices are readable, enter the IP address, netmask and so on, for the back machine.

   Example:

   ```
   linux ip=192.168.0.50 netmask=255.255.255.0 gateway=192.168.0.1 ksdevice=eth0
   ks=nfs:192.168.0.1:/mnt/exports/front.cfg
   ```
4. While running the Anaconda installer, execute the kickstart scripts, then verify *Red Hat Enterprise Linux indicates up and booting* is displayed.
5. Repeat this procedure to install Red Hat Linux on the front machine using another modified version of the kickstart scripts. Remember to enter the IP address for the front machine.

OS configuration

If not using the Avocent-supplied kickstart file, the configuration settings must be set up as follows.

Installation directories

The *Trellis*™ platform is installed to the root by default. If you would like the platform installed to a different location, a symbolic link must be created (as root) to the following folders:

- /u01

- /u02
- /u03
- /u05

User configuration

All *Trellis*™ platform startups, shutdowns, installations, patches and upgrades must be performed using the “oracle” user. The /etc/passwd file should have the oracle user and the SLI user set up and the home directory should be set to “/home/oracle:/bin/bash.”

The "runuser -l oracle -c 'umask'" command returns either 0000 or 0002.

Group configuration

Make sure the oinstall and dba groups in the /etc/group file are set up correctly.

Environmental variables configuration

The following environmental variables should be set for the oracle user:

- PATH should contain /sbin/
- MW_HOME=/u01/fm/11.1.1.7/
- ORACLE_HOME=/u01/app/oracle/product/11.2.0
- ORACLE_SID=orcl

Additional files required

The following file exists with the following permissions set:

- /etc/oraInst.loc = -rw-r--r-- (root)

The /etc/oraInst.loc file contains the following lines:

- inventory_loc=/u01/app/oraInventory
- inst_group=oinstall

The following file exists with the following permissions set:

- /etc/oratab = -rw-rw-r-- (oracle:oinstall)

For Linux 6.x ONLY, the following symlinks should be created and the files exist:

- libcrypto.so.1.0.0 -> /usr/lib/libcrypto.so.10
- libssl.so.1.0.0 -> /usr/lib/libssl.so.10

Additional services required

The /etc/xinetd.d/nodemanager file exists and content is identical to the following:

```
service nodemgrsvc
{
type = UNLISTED
disable = yes
socket_type = stream
protocol = tcp
wait = yes
user = root
port = 5556
flags = NOLIBWRAP
log_on_success += DURATION HOST USERID
server = /bin/su
server_args = - oracle -c /u01/trellis/startNodeManager.sh
}
```

Sudoers content

The "runuser -l oracle -c 'sudo -l' | grep "(root)" command lists out "(root) NOPASSWD:" for the following entries:

- /etc/init.d/trellis
- /u03/root/disable_escalation.sh
- /u03/root/enable_nodemanager.sh
- /u03/root/ohs_enable_chroot.sh
- /u03/root/postinstall_env_setup.sh
- /u03/root/preinstall_env_setup.sh
- /u03/root/sli_install.bin

NOTE: If this cannot be determined, the Sudoers file MUST match engineering specifications, as per the kickstart file.

System settings

The "/etc/sysctl.conf" file MUST contain the required parameters for the *Trellis*™ platform and should meet the following requirements:

- kernel.sem = "250 32000 100 128"
- net.ipv4.ip_local_port_range = "9000 65535"
- fs.aio-max-nr >= 1048576
- fs.file-max >= 6815744
- kernel.shmall >= 2097152
- kernel.shmmax >= 536870912
- kernel.shmmni >= 4096
- net.core.rmem_default >= 262144
- net.core.rmem_max >= 4194304

- net.core.wmem_default >= 262144
- net.core.wmem_max >= 1048586
- kernel.random.write_wakeup_threshold = 1024

The /etc/security/limits.conf file exists and content contains the following:

- oracle soft nproc 2047
- oracle hard nproc 16384
- oracle soft nofile 1024
- oracle hard nofile 65536
- oracle soft stack 10240

The /etc/pam.d/login file exists and content contains the following:

- session required /lib64/security/pam_limits.so

Required packages

For Linux version 6.x the required packages are as follows:

- binutils
- compat-db
- compat-libcap1
- compat-libstdc++-33
- compat-libstdc++-33.i686
- device-mapper-multipath
- dos2unix
- elfutils-libelf
- elfutils-libelf-devel
- emacs fipscheck
- gcc
- gcc-c++
- glibc glibc.i686
- glibc-devel
- glibc-devel.i686
- kexec-tools
- ksh libaio
- libaio.i686
- libaio-devel
- libaio-devel.i686
- libgcc
- libgcc.i686
- libsane-hpaio
- libstdc++

- libstdc++.i686
- libstdc++-devel
- libstdc++-devel.i686
- libXext
- libXi
- libXtst
- make
- openmotif
- openssl.i686
- redhat-lsb
- redhat-lsb-core.i686
- screen
- sgpio
- sysstat
- unixODBC
- unixODBC-devel
- xinetd.x86_64
- java-1.6.0-openjdk
- java-1.7.0-openjdk

NOTE: The Network Manager service should be disabled and the ANT package should NOT be installed.

Security configuration

The following are requirements for configuration of the operating system:

- Disable any Antivirus prior to the installation of the *Trellis*™ platform.
- Disable the Linux® firewall (iptables) and SELinux.
- Make sure the RNGD service is set up to start with Linux® to aid in the generation of entropy. This service is used to generate secure keys used by the *Trellis*™ platform during its execution and installation. Enabling this service dramatically improves the startup performance of systems that typically become starved for entropy.

NOTE: This is even more critical on virtual machines where the system does not generate entropy sufficiently. A hardware TRNG can be used and there are workarounds that offer lower quality entropy; however, use any workarounds with caution.

TRELLIS™ Intelligence Engine hardware requirements and pre-requisites

The following are the minimum deployment requirements for the *Trellis*™ Intelligence Engine. The Intelligence Engine is supported in *Trellis*™ platform version 4.0.3 and higher.

Hardware Requirements

Specification	Datapoints Per Minute				
	10000	20000	30000	40000	50000
CPU Manufacturer	Intel®	Intel®	Intel®	Intel®	Intel®
CPU Model	Xeon®	Xeon®	Xeon®	Xeon®	Xeon®
CPU Speed (GHz) 8M L3 Cache	2.4	2.4	2.4	2.4	2.4
CPU Count	1	1	1	1	1
CPU Cores (per CPU)	2	3	3	4	4
Memory (GB) DDR3 1333 MHz	2	3	3	4	5
Disk Throughput	500 MB/s (sequential) [uncached]				
Storage	25 GB*	35 GB*	35 GB*	50 GB*	50 GB*
Ethernet	>50 MB/s				

* No local backup.

Performance tuning

The following *Trellis*™ Intelligence Engine configuration changes are recommended for instances of the embedded PostgreSQL database where data is collected at 30000 datapoints per minute and higher.

1. Log in to the *Trellis*™ Intelligence Engine host operating system via SSH using PuTTY or a similar program.
2. For RedHat, enter **/var/lib/pgsql/intelligence-engine/postgresql.conf** to open the postgresql.conf file.

   -or-

   For Ubuntu, enter **/etc/postgresql/9.3/intelligence-engine/postgresql.conf**.
3. Use a "vi" editor or similar, enable the following PostgreSQL configuration settings and then adjust the corresponding configuration values as listed:

NOTE: Remove the # symbol for the following configuration settings.

- **shared_buffers** = **256**
- **checkpoint_segments** = **32**
- **checkpoint_completion_target** = **0.9**
- **wal_buffers** = **16**
- **temp_buffers** = **8 MB**
- **commit_delay** = **10000**
- **work_mem** = **16 MB**
- **maintenance_work_mem** = **16 MB**

- **checkpoint_timeout** = **30 min**

4. For RedHat, execute the following commands for the configuration settings to take effect immediately:
    - **systemctl enable postgresql-ie**
    - **systemctl stop postgresql-ie**
    - **systemctl start postgresql-ie**

    -or-

    For Ubuntu, execute the following commands:
    - **/etc/init.d/postgresql stop**
    - **/etc/init.d/postgresql start**

Supported host environments

The *Trellis*™ Intelligence Engine can be installed on VM Ware, Hyper V or a physical machine.

Supported operating systems

The following are the supported operating systems for the *Trellis*™ Intelligence Engine:

- Ubuntu 14.04 LTS (release 14.04.1 and 14.04.3), 64-bit
- RedHat Enterprise Linux (RHEL) 7.2, 64-bit

Supported PostgreSQL databases

The following PostgreSQL databases are installed with the *Trellis*™ Intelligence Engine:

- Ubuntu 14.04 LTS (release 14.04.1 and 14.04.3) – PostgreSQL 9.3
- RedHat Enterprise Linux (RHEL) 7.2 – PostgreSQL 9.2

Installation Tools

To facilitate the installation process, the following tools must be in place on your customer-supplied workstation:

- PuTTY (if installing on Linux and/or planning on upgrading firmware on the Avocent® Universal Management Gateway appliance, to access the front and back machines using SSH via port 22)
- Notepad ++ enhanced text editor (useful if installing on Linux)
- WinSCP (if installing on Linux)
- Windows Sysinternals Toolkit must be installed prior to installation. (Installation is performed by the Professional Services team.)
- PDF Reader and Microsoft Word (to open our installation instructions and copy and paste commands)
- Remote desktop access to both machines (if installing on Windows)

NOTE: Your customer-supplied workstation is not required if the Professional Services team is able to use their workstation to access the *Trellis*™ platform machines while on-site.

Environment Details

The following information must be provided to the Professional Services team before and during the installation process:

- IP addresses and fully qualified domain names for the front and back machines. See Naming Conventions for Platform Domains on page 30.
- Linux root password (or log in as root) or Administrator password for Windows at various points during installation
- Oracle user password (supplied by your Linux administrator when editing the supplied kickstart file)
- Domain and mail server information (to access your SMTP mail server to send mail and to set up new user accounts)

Network Configuration

The following are requirements for network configuration:

- Permanent IPv4/IPv6 addresses are required for both of the *Trellis*™ platform machines (front and back). DHCP is supported as long as the *Trellis*™ platform machines are given specifically reserved IP addresses with permanent leases. Changing the IP address on any of the *Trellis*™ platform machines after installation will cause the application to stop functioning.
- Only one NIC can be enabled for the installation of the *Trellis*™ platform.
- Only one routable IPv4 address can be present/enabled on each platform machine during installation. If there are multiple NIC addresses, they must be teamed so that there is only one routable IP address for the platform machine. Multi-homing is not supported.
- Prior to installation the hosts file (or DNS) must be changed to include the *Trellis*™ platform entries. ALL required hosts names resolve to the correct IP on both the front and back machines.

NOTE: The installation media contains an example configuration for reference.

NOTE: For Windows, entries may be ignored if there are too many entries on any single line of the hosts file. This is an OS limitation.

The front hosts are as follows:

- <FRONT_FQDN>
- <FRONT_HOSTNAME>
- weblogic-admin
- Presentation-Operational-internal
- Presentation-Analytical-internal
- BAM-internal
- SOA-Operational-internal
- SOA-Analytical-internal
- MPS-proxy-internal
- CEP-Engine-internal

  - OHS-Balancer-internal
  - OSB-Server-internal
  - Authentication-internal
  - Authorization-internal-local
  - Flexera-Server-internal
  - vip-external
  - 3rdparty-vip-external
  - vip-internal
  - MPS-proxy-external
  - Search-internal
  - Reporting-internal
  - trellis-front
  - trellis-platform

  The back hosts are as follows:

  - <BACK_FQDN>
  - <BACK_HOSTNAME>
  - MDS-Database-internal
  - CDM-Database-internal
  - TSD-Database-internal
  - TSD-Database-external
  - Authorization-internal-admin
  - trellis-back

- The time server and time zone on the front and back machines should match. In addition, the date and time should match on both machines.

NOTE: This can be omitted if the servers are Domain joined because they will receive time from the Active Directory via NTP.

NOTE: For Linux installations, it is important that the time zone is set to one of the supported time zones. Professional Services can supply a list of supported time zones for the *Trellis*™ platform.

- It is also important to verify that none of the *Trellis*™ platform ports are used by any other running services (see the firewall ports list).
- The *Trellis*™ platform machines should be able to “ping” each other and should return an RTT with 1 hop and < 10 ms RTT.
- The transfer speed between the machines should be > 30 MB/s.

Firewall Ports

The following table provides source and destination components, protocols and ports.

Firewall Ports

Item	Source	Destination	Protocol	Transport	Port	Notes
1	Web Browser	Front Machine	HTTPS	TCP	443	Secure Web UI access
2	Web Browser	Appliance OBWI	HTTPS	TCP	443	Secure Web UI access
			HTTP	TCP	843	Web UI Data - Flash
			HTTP	TCP	8123	Web UI Data - XML
			HTTP	TCP	8080	Upload SSL cert, download backup of the Avocent® Universal Management Gateway appliance, and so on
3	Administrator Workstation	Front Machine (Linux)	SSH	TCP	22	Installation/maintenance access
		Back Machine (Linux)	SSH	TCP	22	Installation/maintenance access
		Appliance	SSH	TCP	22	Installation/maintenance access
		Front Machine (Windows)	RDP	TCP	3389	Remote desktop - Installation/maintenance access
		Back Machine (Windows)	RDP	TCP	3389	Remote desktop - Installation/maintenance access
		Front Machine (Windows)	N/A	N/A	N/A	File copy - Installation/maintenance access
		Back Machine (Windows)	N/A	N/A	N/A	File copy - Installation/ maintenance access
4	Front Machine	Back Machine	ICMP	N/A	N/A	Health check - ping
			TCP	TCP	7	Installation (Jasper) Host validation
			JDBC	TCP	1521	Database
			LDAP	TCP	7023	Security
			LDAP	TCP	7026	Security
			LDAPS	TCP	7027	Security
			TS3	TCP	7031	Security (SSL)
			HTTP	TCP	8080	Entitlement
			SSH	TCP	22	Installation/maintenance access
		Back Machine Windows Only	RDP	TCP	3389	Remote desktop - Installation/maintenance access
		Back Machine Windows Only	N/A	N/A	N/A	File copy - Installation/maintenance access

Item	Source	Destination	Protocol	Transport	Port	Notes
5	Back Machine	Front Machine	SSH	TCP	22	Installation/maintenance access
		Front Machine	ICMP	N/A	N/A	Health check (ping)
		Front Machine Windows Only	RDP	TCP	3389	Remote desktop - Installation/maintenance access
		Front Machine Windows Only	N/A	N/A	N/A	File copy - Installation/maintenance access
6	Front Machine	Appliance	HTTPS	TCP	4440	Communication is one direction but over 2-way SSL
7	*Trellis*™ Intelligence Engine and Appliance	Front Machine	HTTPS	TCP	6443	Communication is one direction but over 2-way SSL
			N/A	TCP	8012	Port used instead of 6443 only if upgraded from *Trellis*™ 2.0.x
8	*Trellis*™ Intelligence Engine and Appliance	Target Devices	SNMP	UDP	161	Set/Get operation, default port; requires customer confirmation
			BACNet/IP	UDP	47808	Default port; requires customer confirmation
			Velocity/IP	UDP	47808	Default port; requires customer confirmation
			OPC UA	TCP	21381	Default port for Matrikon OPC UA Wrapper; default ports for other vendors can differ; requires customer confirmation
			Modbus	TCP	502	Default port; requires customer confirmation
9	Target Devices	Appliance	SNMP	UDP	162	SNMP traps
			N/A	UDP	47777-48117	For BACNet/IP and Velocity return traffic
10	*Trellis*™ Intelligence Engine and Appliance	Service Processors	IPMI	UDP	623	Default port for IPMI
			Telnet	TCP	23	Default port for Telnet
			SSH	TCP	22	Default port for SSH
			HTTP	TCP	80	Used for discovery
			HTTPS	TCP	443	Used for discovery
11	Service Processors	Appliance	N/A	UDP	623	Return IPMI traffic

Firewall Security

Firewall management is extremely resource intensive and requires a high skill level. Because of the effort and complexity involved, a majority of firewall breaches are caused by insufficient firewall rules and policies.

Firewall security is the responsibility of the customer. A top level security policy is essential to any serious security scheme. The policy should outline rules for computer network access, determine how policies are enforced and lay out some of the basic architecture of the company security/network security environment. For your policy, see the National Institute for Standards and Technology for security guidelines.

Provisioning Requirements

The following are the rack U space, power and network requirements for the *Trellis*™ platform components.

Space Provisioning Requirements

Device	Rack U Space Required
Trellis™ platform front and back machines	Based on models
Trellis™ Express Host server	1U
Ntegrity Gateway (NG) appliance	1U
Avocent® Universal Management Gateway appliance	1U

Power Provisioning Requirements

Device	Power Requirements
Trellis™ platform front and back machines	Based on models
Trellis™ Express Host server	2 x 120-220V power supplies
Ntegrity Gateway appliance	1 x 120-220V power supply
Avocent® Universal Management Gateway appliance	2 x 120-220V power supplies

Physical Network Connectivity Provisioning Requirements

Device	Network Requirements
Trellis™ platform front and back machines	Based on hardware
Trellis™ Express Host server	1x
Ntegrity Gateway appliance	1x (optional)
Avocent® Universal Management Gateway appliance	1x corporate LAN (choose 1; 1x empty, 1x teamed corporate LAN, 1x management LAN, 1x private facilities LAN)

Partitions, Disk Space and Permissions

NOTE: The partitions, disk space and permissions requirements are not applicable for the *Trellis*™ Express platform.

NOTE: The following directory structure is representative of post-install utilization; all shown directories are created as part of the installation process. It is not necessary to create the following structures prior to installation.

While the following tables indicate the minimum disk requirement for the application is 300 GB for each server-class machine, the actual disk usage depends on a number of factors, including quantity of data collected and duration of data retention for historical purposes. The following tables illustrate typical disk utilization and are provided as a guideline for planning disk capacity for the *Trellis*™ platform front and back machines.

The minimum disk requirements are for installation purposes only and do not include data collected, duration of data collected or the retention of the data for historical purposes. Please work with the Avocent Professional Services team to plan appropriate disk space for data collection.

Windows Disk Space Usage

Windows Front Machine Application Servers

Directory	Minimum Space Required	Ownership/ Permissions	Content Notes
C:\Users\Administrator	20 GB	administrator	Working directory for installation, upgrades and patching. Examples are: C:\Users\Administrator\AppData\Local\Temp\2 and C:\Users\Administrator\TrellisScripts.zip 10 + GB.
c:\bea\homelist	0.001 GB	administrator	Inventory file for WebLogic installation and patching.
c:\u01	24 GB	administrator	Oracle Tech Stack log files. 99% read only. Logs start at less than 10 GB, but allocate 24 GB for future upgrades of Tech Stack to support log captures and other support-related activities. The execution of capture_logs.cmd places the system state in a zip or jar file in the c:\u01\trellis directory. These small logs are rarely used.
c:\u02	120 GB	administrator	Application Domain/IDM/OHS configuration. Logs start at 7 GB and can grow to 80 GB within six months on an active system. Also, 40 GB are reserved to support patching and support related activities.
c:\u03	5 GB	administrator	Installer logs. In future versions the logs are increased in this location with total space for c:\u02 and c:\u03 remaining the same; c:\u02 space becomes less as logs are placed in c:\u03.
c:\windows\.......	10 GB	administrator	Windows system registry and supporting service initialization.
%CUSTOMER_SPECIFIC_ LOCATION% Windows ISOs	20 GB	administrator	Windows ISOs may be removed after installation of the *Trellis*™ platform or after an upgrade. Avocent currently uses c:\u05 directly internally by convention, but this is customer specific. Space must be allocated for each upgrade and patch.
%CUSTOMER_SPECIFIC_ LOCATION% Binaries	20 GB	administrator	Binaries may be removed after installation of the *Trellis*™ platform or after an upgrade. Avocent currently uses c:\u05 directly internally by convention, but this is customer specific. Space must be allocated for each upgrade and patch.
Reserve	80 GB	N/A	Reserved for contingency.
Total	299.001 GB	N/A	N/A

Windows Back Machine Database Servers

Directory	Minimum Space Required	Ownership/ Permissions	Content Notes
C:\Users\Administrator	20	administrator	Working directory for installation, upgrades and patching: C:\Users\Administrator\AppData\Local\Temp\2; C:\Users\Administrator\TrellisScripts.zip 10 + GB
c:\bea\homelist	0.001	administrator	Inventory file for WebLogic installation and patching.
c:\u01	60 GB	administrator	Oracle Tech Stack log files start at less than 10 GB, but 24 GB are allocated to support future upgrades of Tech Stack for log captures and other support related activities. Execution of capture_logs.cmd places the system state in a zip or jar file in the c:\u01\trellis directory. c:\u01\app\oracle\admin\orcl\dpdump\ contains schema backups.
c:\u02	110 GB	administrator	IDM Domain / Database. Starts at 7 GB and can grow to 80 GB within six months on an active system. Also, 40 GB are reserved to support patching and support-related activities. Database files are stored in c:\u02\app\oracle\oradata\orcl\ grow by design. Calculations must be refined during a sizing exercise.
c:\u03	5 GB	administrator	Installer logs; In future versions of the platform, the logs are increased in this location and totals for the c:\u02 location and c:\u03 location are the same, but the c:\u02 space becomes less as logs are placed in c:\u03.
C:\Program Files\Emerson NetworkPower\	0.2 GB	administrator	License supporting components.
C:\Program Files\Oracle\	0.1 GB	administrator	Oracle Tech Stack inventory and logs of inventory changes.
c:\windows\.......	10 GB	administrator	Windows System Registry and supporting service configuration; 10 GB is aggressive.
%CUSTOMER_SPECIFIC_ LOCATION%\WindowsISOs	20 GB	administrator	Windows ISOs may be removed after the installation of the *Trellis*™ platform or after an upgrade. Avocent currently uses c:\u05 directly internally by convention, but this is customer specific. Space must be allocated for each upgrade and patch.
%CUSTOMER_SPECIFIC_ LOCATION%\Binaries	20 GB	administrator	Binaries may be removed after installation of the *Trellis*™ platform or after an upgrade. Avocent currently uses c:\u05 directly internally by convention, but this is customer specific. Space must be allocated for each upgrade and patch.
%FULL_BACKUP_ LOCATION% %ARCHIVE_ LOGS_DIRECTORY%	5 GB	administrator	Calculations must be refined during the sizing exercise. Generally, this is four times the size of the weekly database backup to be stored and not purged by the *Trellis*™ platform. Growth will depend on the frequency of backups and size of the overall database, as with any log file.
Reserve	80 GB	N/A	Reserved for contingency.
Total	295.301	N/A	N/A

Linux Directories Partitions and Disk Space

You may choose to represent the Linux directories that are required by the *Trellis*™ platform as separate partitions. While this should not introduce any issues with installation, the size of these partitions/directories must be adequate for the installation process. The following table provides requirements for the Linux server team to follow when configuring the directory partitions for the servers on the front and back machines.

Server Directory Partition Requirements

Directory	Minimum Space Required	Ownership/ Permissions	Content Notes
/home/oracle	20 GB	oracle / drwxrwxr-x	Working directory for installation, upgrades and patching; /home/oracle/TrellisScripts.zip 10 + GB profile information.
/tmp	10 GB	root / drwxrwxr-x	/tmp is used during installation; some temp files are placed here during runtime and removed when the server is shut down properly.
/u01	24 GB	oracle / drwxrwxr-x	Oracle Tech Stack; 99% read-only log files starting at less than 10 GB, but 24 GB is allocated for future upgrades of Tech Stack to support log captures and other support related activities; these small logs are rarely used.
/u02	60 GB	oracle / drwxrwxr-x	Application Domain/IDM Domain/Database/OHS configuration. Logs start at 7 GB and can grow to 80 GB within six months on an active system. Also, 40 GB are reserved to support patching and support related activities.
/u03	5 GB	oracle / drwxrwxr-x	Installer logs; in future releases these logs are increased in this location and the \u02 location and \u03 location totals remain the same, but the \u02 space becomes less as logs are placed in \u03.
/u05	24 GB	oracle / drwxrwxr-x	Location for the extracted *Trellis*™ platform installation binaries; used internally by convention as a location to install non-product monitoring services.
/	10 GB	root / drwxr-xr-x	/etc gets populated with scripts to manage the *Trellis*™ platform and Oracle servers.
Reserve	145 GB	N/A	Reserved for contingency.
Total	298	N/A	N/A

Authentication

In addition to one local administrative account, the *Trellis*™ platform supports the following types of user authentication.

- Local user authentication
- Active Directory (AD)
- LDAP

If AD authentication is configured during installation, the Professional Services team needs the following platform information to locate and authenticate users:

- Host: IP address of the domain controller (not the host name)
- Port: TCP port **636** for SSL Mode or TCP port **389** for standard LDAP
- Root: Example - dc=tac,dc=pro
- Base DN, Group Base DN and User Base DN: example dc=tac,dc=pro
- Type: *ACTIVE_DIRECTORY* or *LDAP*
- SSL Mode: Enabled checkbox (use TCP Port 636) or disabled checkbox (use TCP Port 389)
- Access Credentials: Use full username; example cn=Bind,cn=Users,dc=tac,dc=pro

NOTE: Without access credentials, the added external authentication provider may not function as desired.

- Use Chasing Referrals: Enabled or disabled checkbox

Email Notification server assignments

The Email Notification server must be assigned to send temporary login credentials after a user has been created. Temporary passwords are auto generated using the local policy for complexity.

To set up the email notification server to send login credentials:

1. At the *Trellis*™ platform UI, click the *Administration* tab and on the left, select *System Configuration - Server Locations - Email Notification Server*.
2. At the Email Notification Server screen, under Outgoing Server, enable the Use to send SMTP Notifications checkbox and add the following:
   - Mail Server IP/Host: IP Address or FQDN
   - Mail Server Port: TCP Port 25
   - Default Sender: Example - TrellisDCIMAdministrator@tac.pro
   - Mail Protocol: IMAP or POP3

Post Installation - Accessing the TRELLIS™ Platform Online Help File

The help file for the *Trellis*™ platform is available via the Internet. Customers without Internet access or not wanting to expose the *Trellis*™ platform servers to the Internet, can download the *Trellis*™ platform Online Help file for local access. When using a local copy, if you reinstall or upgrade the *Trellis*™ platform software, the location to access the help file resets to the online location and requires resetting to the local source.

To access the *Trellis*™ platform Online Help file from the Internet:

1. In the *Trellis*™ platform UI, click the *Administration* tab and under System Configuration, select *Server Locations*.
2. In the workspace under Help Documentation, verify the View Help from the Avocent web site radio button is selected and click *Download the latest files*.
3. At the Select the Download Source dialog box, select *From the Avocent web site* and click *Download*.

4. In the Server Locations workspace, click *Save - OK*.

To download and install the Online Help file for local access:

1. Using a server with Internet access, visit **http://global.avocent.com/us/olh/Trellis/**.
2. Click *The TRELLIS™ Real-Time Infrastructure Optimization Platform Online Help* and select *Trellis™ Platform Online Help.zip File*.
3. Using a USB drive or CD ROM, copy and transfer the .zip file to the front machine, then in the *Trellis™* platform UI, click the *Administration* tab and under System Configuration, select *Server Locations*.
4. Click *Download Latest Help - From a local source*, browse to the previously downloaded .zip file and click *Download*.

To change the access setting of the online help:

1. From the Administration menu, under System Configuration, select *Server Locations*.
2. Under Help Documentation, select the location of the help file to be accessed and click *Save*.

Network Communication

Different aspects and options must be considered when installing the *Trellis*™ platform on a network, both externally and internally.

The application servers must be able to communicate externally with Avocent entitlement servers during installation and any time licensing or entitlement is changed. SSL-secured communications use port 443 from the application servers to access: https://licensing.emersonnetworkpower.com/entitlementhub/ActivationService.svc.

Internally, application servers may communicate with each other and with Universal Management Gateway appliances when one or more appliances are part of the platform and reside on the same network and/or subnet. A key strength of the platform is this ability to connect to a vast array of infrastructure devices to gather information. Connectivity is primarily provided by the *Trellis*™ Intelligence Engine, Avocent® Universal Management Gateway appliance or the Liebert® Ntegrity Gateway appliance.

Communication with devices is via public or private networks or via physical connections. Each engine/appliance has two main network ports, eth0 and eth1, and at least one of these two ports must be able to communicate on a LAN network to the application servers.

Each engine/appliance supports physical and logical connections to target devices.

NOTE: Only one engine/appliance is allowed to be connected to and monitor a target device at the same time.

Avocent® Universal Management Gateway Appliance

The Avocent® Universal Management Gateway is an optional multi-purpose appliance that offers consolidated access to facility and IT equipment, making it possible for data centers to execute a unified approach to infrastructure management, and resulting in greatly reduced cost and more efficient management and control. The appliance solves problems in the data center infrastructure management (DCIM) market by providing both real-time data and closed loop control to the *Trellis*™ platform solution. Within DCIM, remote data center management (RDCM) has been defined as IT access and control.

Ntegrity Gateway Appliance

The Ntegrity Gateway appliance is an optional secure hardware appliance that resides within the enterprise private network to collect information from devices being monitored and provide remote access to other *Trellis*™ platform hardware. This is a very useful tool in situations where customer support is required, allowing Avocent Technical Support to access the *Trellis*™ platform hardware to assist with upgrades or other support related matters.

For more information about appliances, please contact your sales person.

Logical connections

Targets connected to an appliance logically are available via network access, which has several options.

Service processor (SP) targets

SPs may be logically connected to an appliance using an SP sub-network, or they can be connected logically or physically via appliance target ports.

SP sub-network

The appliance may be connected to the SP sub-network using the eth1 port of the appliance. This setup is recommended when OEM tools, such as HP, SIM or IBM Director, are already being used and must also have network access to the SPs.

Logical connections via appliance target ports

The appliance may connect to SPs logically or physically via one or more of the target ports, if the ports are connected to a customer network. Each SP in this configuration requires a dedicated appliance target port.

Monitoring targets

To monitor targets via a logical network connection, one of the two dedicated Ethernet ports on the appliance, eth0 or eth1, must be connected to that network.

Physical connections

Targets must be connected to one of the target ports on the back of the appliance. Different appliance models have different port configurations.

KVM

When supported, a KVM target requires use of a UMIQ module and must be connected to the appliance by an Ethernet cable with a total length not longer than 100 m.

CAUTION: Never connect a network switch, hub, firewall, router or anything, between an appliance and a UMIQ module. Appliances send electricity that damages anything that is not a UMIQ module.

Other targets, such as the SP or serial console

NOTE: Depending on the appliance model, other targets may be physically connected to the proper appliance ports. Monitoring of facilities equipment, such as PDUs or UPSs, is only supported via logical network connections.

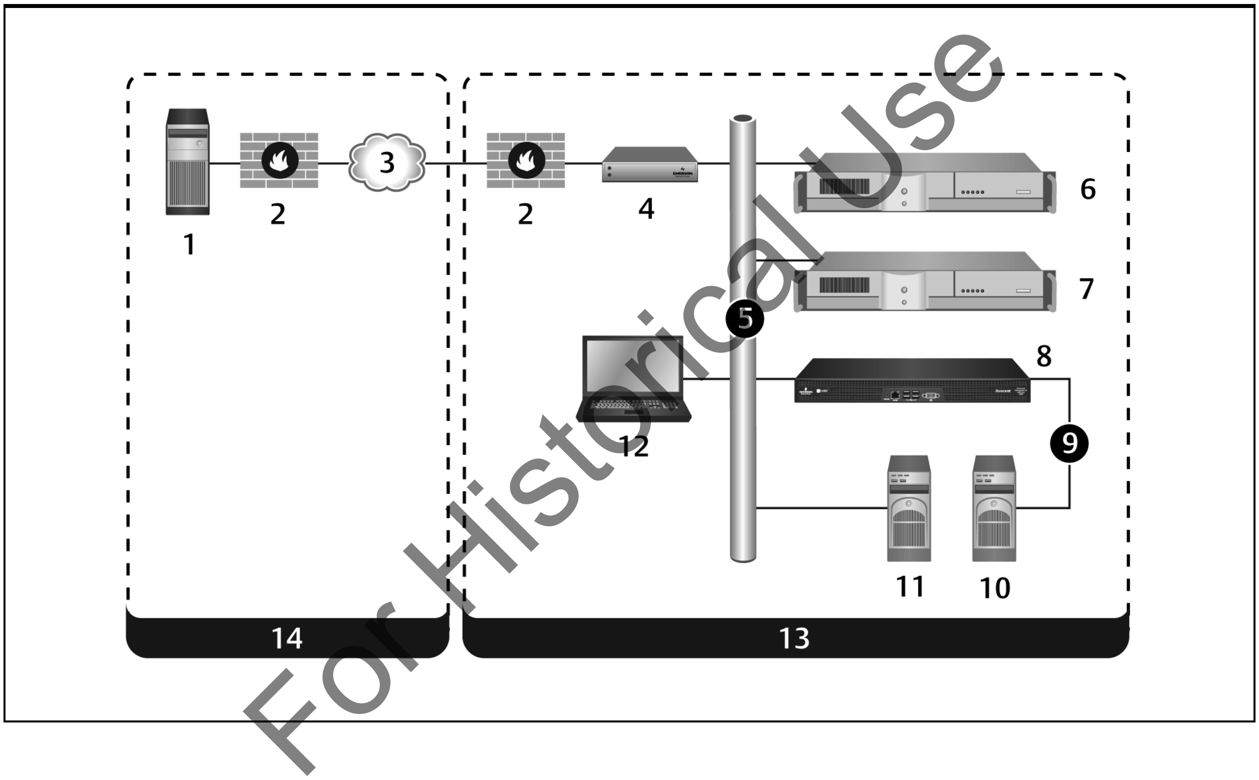
Common Installation Scenarios

Various options are available when deploying the *Trellis*™ platform with the Avocent® Universal Management Gateway and Ntegrity Gateway appliances. The Avocent® Universal Management Gateway appliance is placed behind the firewall. The Ntegrity Gateway appliance may be placed in a DMZ or behind a firewall. For deployment scenarios using the Ntegrity Gateway appliance behind a firewall, see Installation on a Network on page 25. Facilities equipment within the data center may reside on a corporate network or on a private network. For scenarios where facilities equipment is on the corporate network, see Installation on a Network on page 25 and Installation on a Separate Private Network for Facility Equipment on page 26. For an example of devices on a private network, see Installation on a Separate Private Network for Facility Equipment on page 26.

Installation on a network with the Ntegrity Gateway appliance

In this scenario, the platform is installed on the front and back machines, which are accessed by a user with a web browser on the same corporate LAN. The Ntegrity Gateway appliance is behind a firewall communicating to Emerson Network Power via a secure connection. The Avocent® Universal Management Gateway appliance is on the same corporate LAN as the platform machines, monitoring physical target devices such as power strips and PDUs on that same network. Some devices may also be physically connected to ports on the back of the Avocent® Universal Management Gateway appliance.

Installation on a Network



Installation on a Network without Facilities

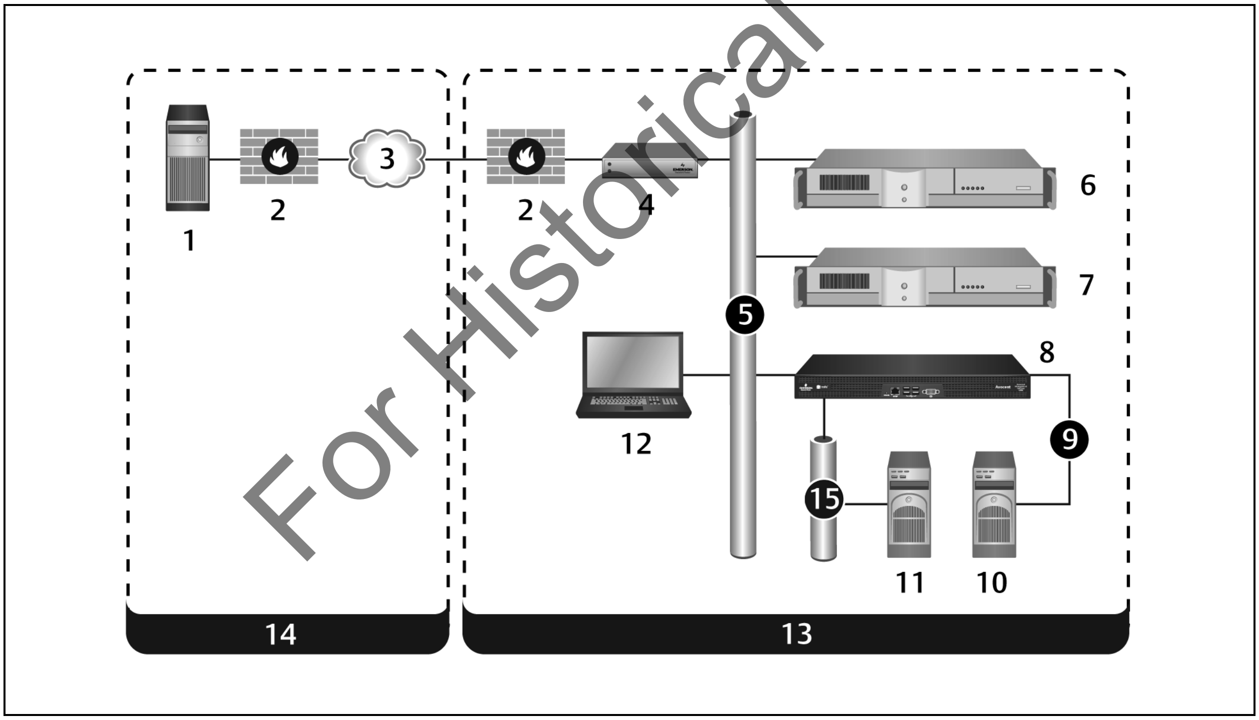
Item	Name	Description
1	Emerson Controlled Access Server	Provides network security enforcement
2	Firewall	Prevents unauthorized access to or from a private network
3	Internet	Global system of interconnected networks
4	Ntegrity Gateway (NG) appliance	Ensures the security of a network
5	LAN	Computer network that interconnects computers within a limited area
6	The *Trellis*™ platform front machine	The software platform production system front end
7	The *Trellis*™ platform back machine	The software platform production system back end
8	Avocent® Universal Management Gateway appliance	Enables remote management of devices

Item	Name	Description
9	Serial Over Ethernet	Allows for sharing a serial port over the network (Internet or LAN)
10	Physical Target Devices	Represents the physical target devices
11	Logical Target Devices	Represents the logical target devices
12	Users	The *Trellis*™ platform users
13	Unencrypted Local Traffic	Local traffic that is unencrypted
14	Encrypted Network Traffic	Network traffic that is encrypted

Installation on a separate private network for facility equipment

In this scenario, the Ntegrity Gateway appliance sits in behind a firewall and facilities equipment is logically connected on a private facilities LAN. To access the private LAN, the Avocent® Universal Management Gateway appliance is dual-homed. Some devices may also be physically connected to the ports on the appliance.

Installation on a Separate Private Network for Facility Equipment



Installation on a Network with Facilities

Item	Name	Description
1	Emerson Controlled Access Server	Provides network security enforcement
2	Firewall	Prevents unauthorized access to or from a private network
3	Internet	Global system of interconnected networks
4	Ntegrity Gateway (NG) appliance	Ensures the security of a network

Item	Name	Description
5	Corporate LAN	Computer network that interconnects computers within a limited area
6	The *Trellis*™ platform front machine	The software platform production system frontend
7	The *Trellis*™ platform back machine	The software platform production system backend
8	Avocent® Universal Management Gateway appliance	Enables remote management of devices
9	Serial Over Ethernet	It should be noted that this is only a sample and assumes that the backup location provides an ssh interface, and allows for the exchange of SSH keys
10	Logical Target Devices	Represents the logical target devices
11	Physical Target Devices	Represents the physical target devices
12	Users	The *Trellis*™ platform users
13	Unencrypted Local Traffic	Local traffic that is unencrypted
14	Encrypted Network Traffic	Network traffic that is encrypted
15	Facilities LAN	Provides a computer network that interconnects computers within a specific area

Configuring BACnet devices

When an appliance such as SiteLink™, is monitoring Building Automation and Control Networks (BACnet) devices, and it is on a different IP subnet than the subnet that the Avocent® Universal Management Gateway appliance is on, the IP address of the SiteLink appliance needs to be added to the BBMD (BACnet Broadcast Management Device) table for the BACnet router on that IP subnet.

A SiteLink appliance is always a BACnet device and can also be a BACnet router. For SiteScan™, one SiteLink per subnet is automatically configured as a BACnet router (or BBMD) when the system is built. That is how SiteScan (an IP-based system, often on a separate subnet from one or more SiteLink appliances) works.

When adding the appliance to the network, this BACnet router SiteLink requires the IP address of the appliance to be appended in its BBMD table. If the appliance is accessing other SiteLink appliances on the same subnet, which were not originally BBMD routers, those SiteLink appliances may also need to be forced to act as a BBMD. BACnet should function with only one BBMD per subnet, which acts as a router for all other BACnet devices on the subnet. The *Trellis*™ platform supports this by allowing you to enter the IP address of both the monitored SiteLink appliance and the appropriate BBMD router. For SiteLink appliances that are also configured as BBMD routers, both of these addresses are the same.

There are ways to update the existing BBMD tables on SiteLink hardware through SiteScan, as well as using separate software tools. These are generally proprietary/vendor-specific.

NOTE: Customers may have BACnet systems that are not SiteScan/SiteLink devices.

Best practices for Virtual Machine (VM) environments

The following best practices help ensure optimal performance when running the *Trellis*™ platform in a virtual environment.

- If power management is enabled on the host machine BIOS, disable it, then in the processor settings, disable *C-States* and *C1E* and set the power management settings to *Maximum Performance*.
- Always use the minimum recommended resources in the *Trellis*™ platform VMs.

NOTE: Depending on the density of the cluster that is housing the *Trellis*™ platform, if there is a high vCPU/pCPU ratio on the hosts, we have seen CPU ready times > 200-300 ms cause a drop in performance. For this, we recommend adding more hosts to counteract CPU contention. If this is not possible, we have seen a considerable drop in CPU contention and better performance when dropping the VMs from four vCPUs to two vCPUs.

- If resources are overallocated, or if there is contention, make sure to have the VMs in a resource pool with high memory/CPU shares and set reservations when possible.
- When taking a snapshot of the *Trellis*™ platform VMs, make sure the platform services are stopped or the VMs are powered off to ensure the VMs are in sync for the snapshot and to avoid failures due to high amounts of I/O traffic.
- Do not run VMs that are housing the *Trellis*™ platform on snapshots for extended periods of time. The delta files can grow rapidly due to the amount of I/O in the *Trellis*™ platform. This also decreases read/write speeds and causes performance degradation.
- If you are using Distributed Resources Scheduler (DRS) and the VM network traffic becomes a bottleneck, set affinity rules to keep the front and back VMs on the same host.

Appendices

Appendix A: Browser Recommendations

The following are general recommendations pertaining to the supported browsers:

- If on-screen data is not updating correctly, clear the browser cache.
- If security certificate warnings are displayed while using an https connection to access the *Trellis*™ platform, ignore the warning and proceed to access the site.
- Disable pop-up blockers.
- If accessing graphical pages, use Adobe Flash Player version 12.0 or higher.
- When importing or exporting data using Internet Explorer, select *Tools - Internet Options - Advanced*, then under the HTTP 1.1 settings section, deselect *Use HTTP 1.1*.
- When using Reports and establishing a secured connection (https) using Firefox, if the browser does not have the latest certificate installed (particularly while installing newer builds), manually delete the old certificate and re-launch the application.

Appendix B: Naming Conventions for Platform Domains

When assigning a domain name to the *Trellis*™ platform, the following are required:

NOTE: The *Trellis*™ platform domain name is not an FQDN name.

- The domain name should be alphanumeric with no spaces or special characters.
- If the name begins with t, b, n, r, or f, the initial character must be capitalized to prevent the name from being confused with various specific commands/sequences in the software.
- If running multiple *Trellis*™ platform instances on the same network segment, each *Trellis*™ platform domain name must be unique.
- The domain name should begin with an alpha character and have 16 or less characters in the name. The following are examples of acceptable names:
    - TrellisDomain
    - TrellisPROD
    - TrellisLIVE
    - TrellisDEV
    - TrellisTEST
    - TrellisPRODDomain
    - LIVETrellisDomain
    - TrellisDEVDomain
    - TESTTrellisDomain

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. For additional assistance, visit www.vertivco.com/en-us/support.

Avocent Community Support Site

To search product knowledge content,
visit https://vertivco-eng.custhelp.com/app/community/page/1.

About Emerson Network Power

Emerson Network Power, a business of Emerson (NYSE:EMR), delivers software, hardware and services that maximize availability, capacity and efficiency for data centers, healthcare and industrial facilities. A trusted industry leader in smart infrastructure technologies, Emerson Network Power provides innovative data center infrastructure management solutions that bridge the gap between IT and facility management and deliver efficiency and uncompromised availability regardless of capacity demands. Our solutions are supported globally by local Emerson Network Power service technicians. Learn more about Emerson Network Power products and services at **www.EmersonNetworkPower.com**.