KMCDome™

Cybersecurity Powered by Veridify

DOME Installation Guide

928-035-02B

Do you find this document helpful?
Click here to share feedback and help us improve:
Give Feedback

KMC Controls, 19476 Industrial Drive, New Paris, IN 46553 / 877-444-5622 / Fax: 574-831-5252 / www.kmccontrols.com

Proprietary Notices

1. Legal Disclaimer

The use of DOME is subject to Veridify's standard license terms and conditions as set forth in the DOME Building Automation Starter Kit - Proprietary Notices; License Terms and Conditions ("Standard Terms"), as well as the Software-as-a-Service Agreement. This documentation does not expand or otherwise modify Veridify's Standard Terms or mutually, in writing, agreed upon terms, including, but not limited to, the disclaimers and warranties expressed therein.

2. Copyright Notice

Third-Party notices, terms, and conditions pertaining to third-party software and hardware can be found at:

https://www.veridify.com/terms-of-use/

3. Trademark Notice

The KMC Dome Cybersecurity Powered by Veridify logo is the trademark or service mark of KMC Controls. Device Ownership and Management Enrollment, and DOME are trademarks or service marks (individually and collectively, "Marks") of Veridify Security Inc. ("Veridify"). The Marks displayed in this documentation or on any hardware or in any software represent some of the proprietary rights currently owned or controlled by Veridify and are not intended to be a comprehensive compilation of all Veridify's worldwide proprietary ownership rights. See, https://www.veridify.com/terms-of-use/ for representations of additional Marks owned or controlled by Veridify and additional guidance with respect to Veridify Marks. All other trademarks and service marks, which may be registered in certain jurisdictions, belong to the holder or holders of such marks.

4. Patent Notice

DOME is protected by certain patents. In accordance with the virtual marking provisions of the American Invents Act, 335 USC 287(a), See, https://www.veridify.com/terms-of-use/, which enumerates the list of products and components that may be protected by one or more patents, or patents pending in the US and elsewhere. Certain third-party components embedded in DOME may be protected by certain patents of such third party; reference should be made to the third-party documentation.

Contents

DOME Components

DOME User Panel™ (DUP)	System for installation set-up and device management
DOME Dashboard™	Dashboard for system information, analytics, and alerts.
DOME Interface Appliance™ (DIA)	Local management device at an installation being protected
DOME Sentry™ devices	Security appliance that protects edge devices
DOME Mobile App™	Mobile app for registering DOME Sentry devices

Installation Checklist

Planning for these item will help to quicken the installation of DOME. Please visit the sections below for each action prior to installation.

✓	**Action**
	Complete a Site Survey for each building (Section 1.2) It is recommend to use Veridify's site survey document "DD-0028 Site Survey Form"
	Register for a DOME Account (Section 1.1) https://dome.veridify.com/signup See "DD-0036 DOME Account Reference Guide" for screen details Note - This applies only to the first person in a new system integrator organization, everyone else will receive an email invitation to create an account.
	Log-in to your DOME Account to verify set-up is compete https://dome.veridify.com/manage
	Gather Network Address information for DIA (Sections 1.2 and 2.4)
	Gather the following items for installing the DIA (Sections 2.2 and 2.4) • HDMI monitor and cable • USB keyboard and mouse • Power and network connectivity (10/100/1000Mbps) • One or two Ethernet cables (depending on configuration)
	Install the DOME Mobile App (Section 3.2) – available for iOS and Android https://www.veridify.com/apps
	Ensure that devices are discoverable on the network • Power on if not operating due to seasonal-use only • Enable BACnet on JACE controllers and ensure the BACnet driver is associated with the active network interface

1. Pre-Installation Planning

1.1 DOME Account Registration

A DOME account for the installing organization must be set up and approved prior to installation of the DIA. The first person in a new system integrator organization installing DOME will register a new account as listed in the following steps. Everyone else associated with the installation, including technicians, engineers, facility managers, and facility owners, will receive an email invitation to create an account.

Step 1 – Register for a DOME account at **https://www.veridify.com/install**
Step 2 – Verify your email address from an email the system will send to you
Step 3 – Notification of approval will be sent by email after Veridify approves the account

See document "DD-0036 DOME Account Reference Guide" for registration process and screen details.

Note - Approval by Veridify is not a real-time process. It is recommended that you register for your account several days prior to installation of DOME. Once an account is approved, all subsequent users invited from that account are automatically approved.

1.2 Information Requirements

A DOME Site Survey records information on the networks and devices installed in buildings that will become a DOME site. To accommodate larger DOME installations, Sentry devices will likely be installed in 'pass-through mode' (Not Secure). Once all Sentry devices are physically in place and online, the site configuration will be updated to turn off 'pass-through mode' via the DOME Interface Appliance (DIA), making the site "Secure."

To plan for the installation of DOME, after the site surveys are completed, additional information from the customer may be needed. Below is the list of additional information that will be needed, why it is needed, and how to use it.

Information for the following items is needed:

- DIA IP Address(es) and configuration method (static or DHCP)
    - LAN-A
    - LAN-B
- DIA Console Access Mechanisms
- OT Network Address(es)
- IP Gateway Addresses or Rules for Sentry network(s)

The Sentry device can determine its IP Address and MAC Address from the device it protects, however it cannot determine the Network Size (CIDR / Netmask) nor IP Gateway/Router on its own. To solve this issue, the Sentry device was designed to use mDNS (Multicast DNS) to request this information from the DIA. The DIA is configured with the network/CIDR and gateway information in order to respond to the Sentry device requests.

Note - When a Sentry device cannot reach the DIA via mDNS, the information it would acquire from mDNS can be pre-programmed in. Please see section 3.5 for instructions on how to pre-configure a Sentry device for an environment where mDNS is unavailable.

DIA IP Address(es): This information is needed in order to configure the DIA. It must have a stable address that the Sentry device can reach, regardless of whether that address is acquired via DHCP or statically configured. If the DIA is being installed with two network addresses, only the OT network needs to be static. Record the DIA IP address the Sentry devices will use to talk to the DIA.

DIA Console Access: The DIA is the management console for the DOME Installation and is used to reconfigure and push out provisioning changes to the Sentry devices. An authorized User will need to access and log into the DIA to perform these tasks. Typically, a User will log in via the DIA device console (using an attached keyboard, mouse, and monitor). However, if the DIA is installed in a Data Center, the User may need to use a remotely accessible KVM that will then give them access to the console.

OT Network Addresses(es): This is the list of network addresses of the devices the Sentries will protect. This information is part of the DOME site surveys. The DIA will need to be configured with the list of all networks in CIDR format.

Example 1 - If an existing device is at 192.168.5.23/24, then that is one of the networks for the list (the "24" is the CIDR size, and the DIA will convert this IP Address to the proper network address, 192.168.5.0/24).

Example 2 - If the device address is: 10.20.30.40 netmask: 255.255.252.0, this pair translates to a CIDR size of 22 (10.20.30.40/22). A website like https://dnschecker.org/netmask-cidr.php can help translate from netmask to CIDR size.

Go through all the site surveys to determine the full list of networks and CIDR size(s).

IP Gateway Addresses: There will be multiple routed networks connecting devices except in smaller installations. Each Sentry device needs to learn (or be told) its router address, and each OT network input into the DIA can be individually configured with its gateway. This will enable the DIA to announce the gateway to the Sentry device.

IP Gateway Rules: In the case where mDNS is not usable, the Sentry device can be pre-programmed with an IP Gateway Rule. The Sentry device currently supports two Router Rules: ".1" and ".254" and the appropriate rule to use is determined by the installation environment:

- The ".1" rule tells the Sentry device to compute the lowest IP Address on the network and use that as the router. For example, if the network is 192.168.5.0/24, the ".1" router will be 192.168.5.1. If the device IP is 10.40.80.100/29, the network is 10.40.80.96/29, then the router will be computed as 10.40.80.97.
- The .254 rule tells the Sentry device to compute the highest IP Address on the network and use that as the router. For example, if the network is 192.168.5.0/24, the ".254" router will be 192.168.5.254. If the device is 10.40.80.100/29, the network is 10.40.80.96/29, then the router will be computed as 10.40.80.102.

2. DOME Interface Appliance

An “Installation” needs to be created for each DIA. An Installation can be a single building or a collection of buildings.

2.1 Create Installation Process

1. Log in to your DOME account at https://dome.veridify.com/manage
2. Register the Installation by providing details about the location.

The following information will be required:

- Owner (organization) name and address
- Contact information for at least one owner representative (name, title, email, phone)
- Site name and address

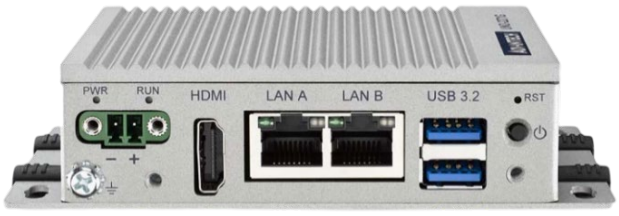
3. Proceed to the installation location for the remaining steps.

2.2 Installation and Configuration Requirements

Installation and configuration of a DIA requires the following items:

- DOME account
- HDMI monitor and cable
- USB keyboard and mouse
- Power and network connectivity (10/100/1000Mbps)
- One or two Ethernet cables (depending on configuration)

2.3 DOME Interface Appliance



DM-ADVT-2271

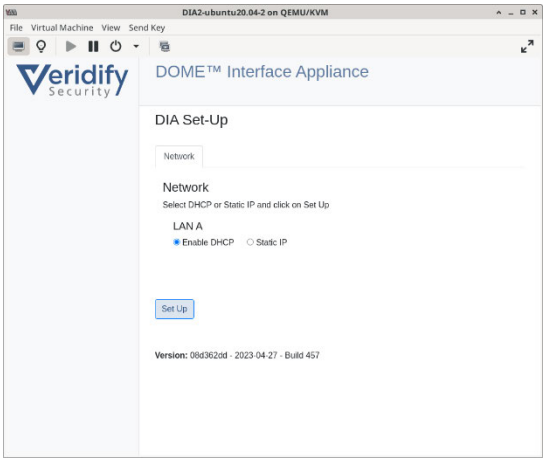
2.4 DIA Installation Steps

Pre-Installation

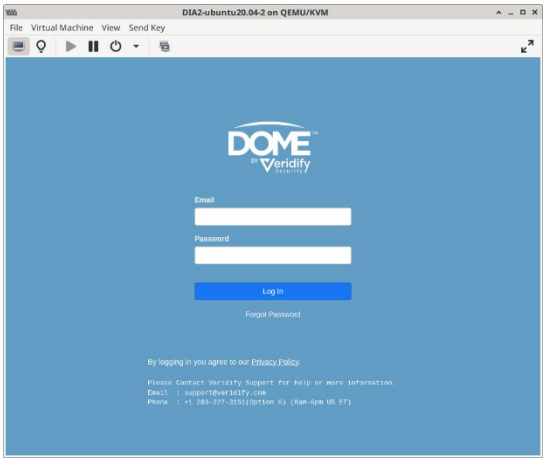
The DIA should operate whenever power is applied without the need to push the power button. This is enabled by a hardware jumper setting and should be adjusted, verified, or tested before installation. Remove the bottom cover and look for the jumper pin header labeled PSON1. Set the jumper to connect pins 1 and 2. When the jumper is set to connect pins 2 and 3, the power button must be used to turn on the device, including after a power outage.

All steps are summarized here with screenshots for steps 6-13 below:

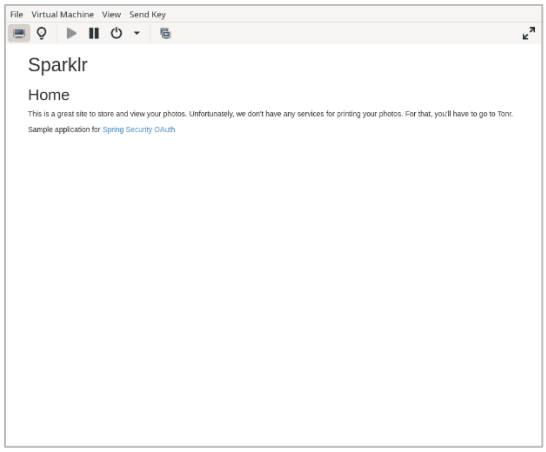
1. Mount the DIA.
2. Connect the network to DIA port LAN A, and optionally LAN B if being used.
3. Connect monitor, keyboard, and mouse.
4. Connect power to the DIA and monitor.
5. Turn on the monitor and the DIA (if it does not automatically turn on check the jumper if needed).
6. Follow the on-screen instructions to get the DIA onto the network by selecting DHCP or Static IP (network information required).
7. Log in to your DOME account *.
8. Select the installation and select “OK” when prompted.
9. The DIA will reboot.
10. Log in to your DOME account again to finish set-up.
11. Go to tab “Network Configuration” to configure the network settings.
12. If two networks are being used, go to tab “OT Configuration” to configure the list of available OT Networks available to the Sentry devices.
13. Go to tab “Sentry Configuration” to set the Sentry device firewall configuration.



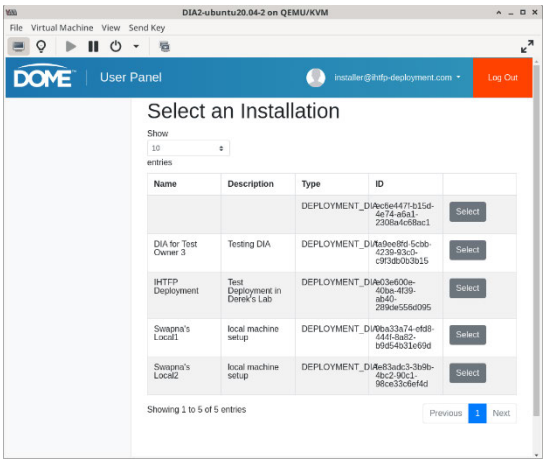
Step 6 – Network Setup



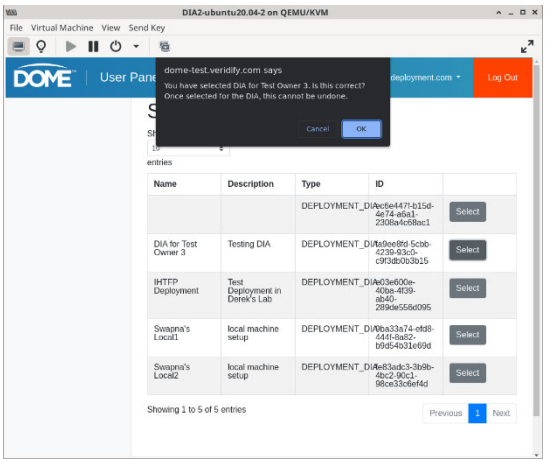
Step 7a - Login



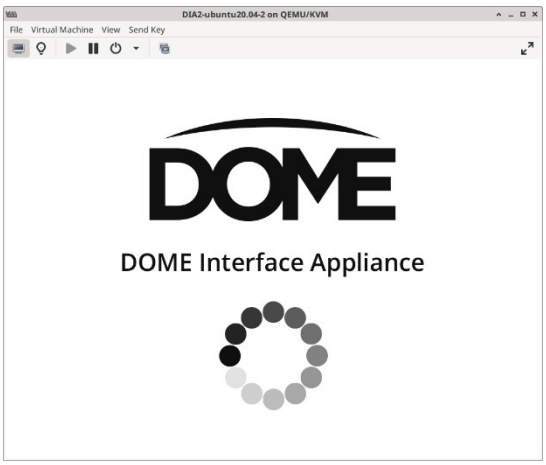
Step 7b – Sparklr page – if the DIA log-in screen is left active for an extended period of time, the system may timeout and provide the page above when trying to log in. Please use Ctl-W to reboot the browser and continue to log-in.



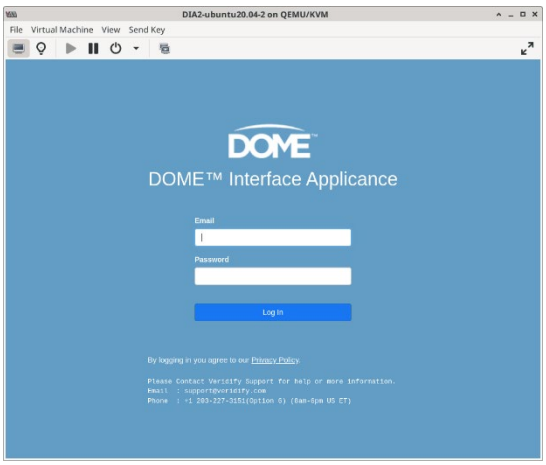
Step 8a - Select Installation



Step 8b – Confirm Selection



Step 9 - Reboot

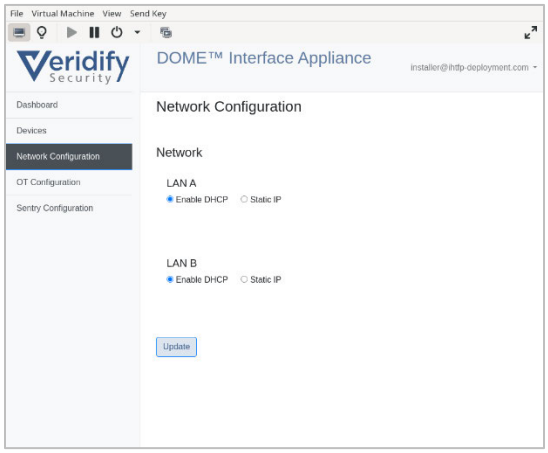


Step 10 - Login

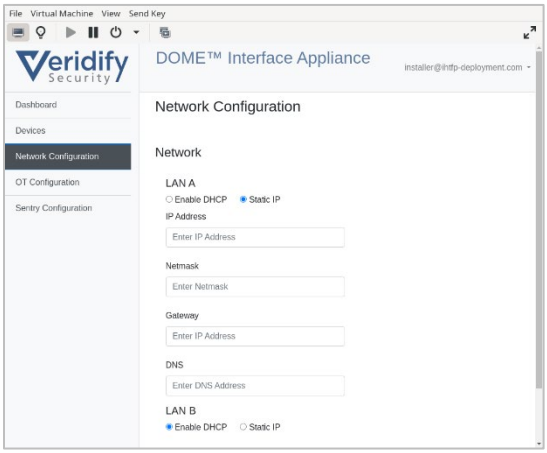
Step 11 - DIA Network Configuration

The DIA supports connectivity to two networks – one for internet access and one for OT devices. If these are both on the same network, then only LAN A is needed. At least one interface must be configured as a static IP address.

Network Design	Configuration Settings
Single network for Internet access and OT devices	Use LAN A port (must select “Static IP” and provide the required network address information)
Separate network for Internet access and OT devices	LAN A – for network with Internet access (DHCP or Static IP is acceptable) LAN B – OT network (must select “Static IP” and provide the required network address information)



Step 11a – DIA DHCP Network Configuration

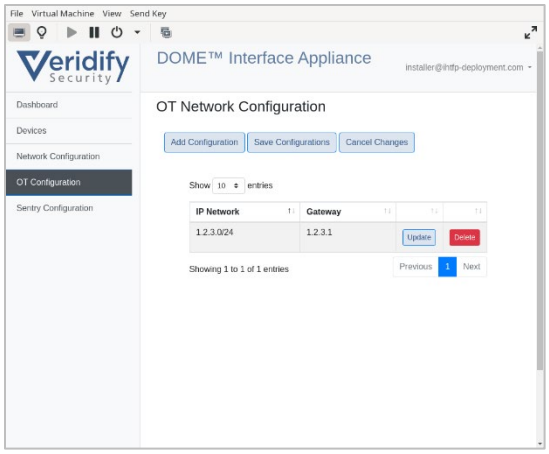


Step 11b – DIA Static Network Configuration

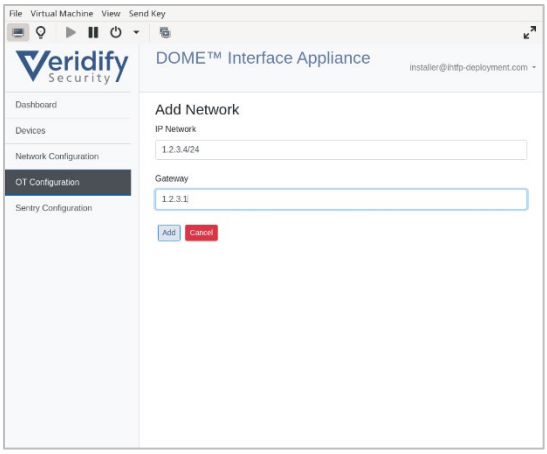
Step 12 – OT Network Configuration

This page controls the OT network configurations when Sentry devices will be installed on a network without internet access. For each possible Sentry OT Network, the IP address, network size are required, while the network gateway address is optional. In smaller installations, the Sentry device will acquire this data directly from the DIA during its auto-configuration step, which is why this data must be in place. The DIA also uses this information to ensure the routing table enables the DIA to reach the Sentry device networks through the appropriate Network Interface configured in the previous step.

Saving changes is required after adding or deleting a configuration for those changes to take effect.



Step 12a – OT Network Configuration



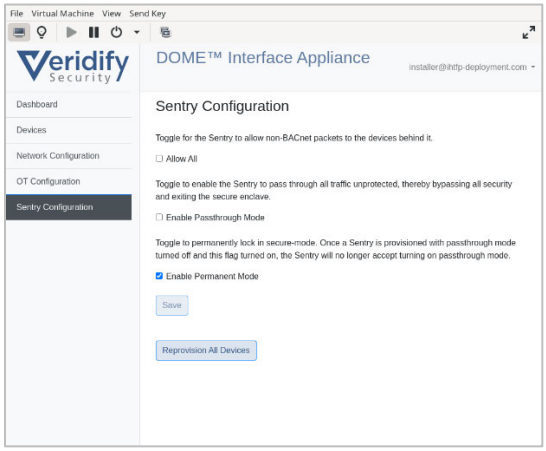
Step 12b – Add OT Network

Step 13 – Sentry Device Configuration

This page controls the settings that are provisioned onto every Sentry device managed by the DIA. You must explicitly save any changes for them to take effect. Once saved, these settings will be applied to any Sentry device that comes online after the settings are made. To push the changes to deployed Sentry devices, use the "Reprovision All Devices" button after saving the configuration.

There are three settings for configuring the capability of a Sentry device.

Allow All	This is for BACnet devices and allows for non-BACnet traffic to also pass to the protected device.
Enable Pass-through Mode	This allows for installing Sentry devices and letting the network operate without security.
Enable Permanent Mode	This permanently activates the security function of the Sentry device and Pass-through Mode will no longer be allowed to be selected.



Step 13

Peripheral Devices
After configuration is complete, the monitor, keyboard, and mouse can be disconnected if desired, but they can remain as part of the DIA installation. They will be needed again to change the settings (e.g. to convert from Pass-through to Secure mode).

Sentry devices can now be registered through the DOME Mobile App and then installed.

2.5 DIA Operation

After installation and set-up, the DIA is not involved in the continuous operation of security. DOME-enabled devices, including Sentry devices, communicate between themselves without the DIA.

After DOME-enabled devices are provisioned onto a network, the DIA is required for the following functions:

- log aggregation
- alerts and notifications
- Sentry device management
- Certificate and Key management & Refresh
- Sentry device software updates
- Firewall and whitelist updates
- Protected device maintenance/modifications (e.g. replacing BACnet IP hardware)

The DIA automatically refreshes Sentry Certificates so they do not expire. If a certificate is left to expire (e.g. DIA not available), the Sentry device and other DOME-enabled devices will be unable to communicate.

At this time, if a DIA fails, a replacement DIA will need to be created by Veridify and then it can be physically deployed to replace the failed DIA.

3. Sentry Device

3.1 Sentry Device

DM-SENTRY-NANO-BAC or DM-SENTRY-NANO-TCP

Port Assignment

Network Port(s)	LAN1, LAN2
Device Port	WAN
USB Port(s)	Config only
HDMI port	Not used
SD slot	Not used
SIM slot	N/A
Antenna port(s)	N/A
RST (Reset)	Not used
Mask	Not used

Note – The Sentry device has three network ports. LAN1 and LAN2 can be used for deployment in a daisy-chain configuration. The WAN port is connected to the device to be protected.

Sentry Device Power Connections

USB with USB-C connector (5V DC)

Pin Label	Description
+Vs	PWR V+ DC power input PIN
GND	PWR V- DC power input PIN
⏚	GND

3.2 Sentry Device Registration

The Sentry devices must be registered in order to operate. Only registered Sentry devices can communicate with the DIA and other registered Sentry devices.

Before Registration

1. Install the DIA as described above. Sentry device registration cannot proceed without the DIA registered to an Installation as described in section 2.

2. Install the DOME Mobile App™ on your mobile device (Internet connectivity is required when using the app). The app is available for Android and iOS. (https://www.veridify.com/apps)

Register devices with the DOME mobile app

1. Open the DOME mobile app.
2. Log in with your DOME account.
3. Select "Register Devices".
4. Select an Installation.
5. Scan the QR code on the Sentry device from the label that has the Veridify Security logo.
6. Add optional device and location information into the app and submit the data.
7. Repeat as needed until all Sentry devices are registered.

Register devices online

1. Log in to your DOME account at https://dome.veridify.com/manage.
2. Click on "Register Device" on the Home screen.
3. Enter the manufacturer's Serial Number of the device (not Veridify S/N).
4. Repeat as needed until all Sentry devices are registered.

You can log in to your DOME account to verify if the Sentry devices are registered.

3.3 Sentry Device Installation

The Sentry device is designed to auto-configure itself when it is connected. It requires the DIA to already be online and running, and it depends on the DIA to provide some network configuration information as well as the required security information the Sentry device needs to connect to the network.

1. Ensure the device to be protected is installed, powered on, and operational before the Sentry device is connected and powered on.
2. Mount the Sentry device (DIN rail, wall, etc.) as close as possible to the device to be protected.
3. Remove the network cable from the device to be protected and plug it in to the Network Port on the Sentry device.
4. Add a cable to connect from the Device Port on the Sentry device to the ethernet port on the device to be protected.
5. Attach the power connection to the Sentry device.

The Sentry device will auto-configure itself to the network and there is nothing further to do. The tables below show the states the Sentry device goes through for configuration and the corresponding LED indicators.

Sentry device Configuration States and LED Indicators

LED State	SYS	WAN	LAN (1&2)*
Power On	Flash	Off	Off
Ready to Provision	Flash	On	Off
Found Device / Getting Network Parameters	Flash	Flash	Off
Failed to Get Network Parameters	Flash	Flash	Flash
Got Network Parameters / Contacting DIA	Flash	On	Flash
Communicating to DIA	Flash	Off	Flash
Provisioned / Running Insecurely (Protection OFF)	Flash	Flash	On
Provisioned / Running (Protection ON)	Flash	On	On

*Note: The LEDs 1 and 2 reference the LAN ports being used.

3.4 Device Configuration – Connecting to the Console Port

Certain limited Sentry device configurations can be made through a connection to a USB port or console port on the Sentry device. The commands are described in the next section.

DOME Sentry Devices

A crossover USB cable is needed to connect from your computer to the Sentry device. The cable is part of the KMC Dome Sentry Starter Kits (DM-START-NANO-BAC and DM-START-NANO-TCP) and can also be purchased separately (DM-SENTRY-USB).

Connect the crossover USB cable to any USB port on your computer and any USB port on the Sentry device.

The terminal emulator should be set to: 115200 bps, 8 data bits, 1 stop bit, no parity, no flow control.

3.5 Device Configuration – Sentry Device Commands

Configuring a Sentry device can be automatic or manual depending on certain models or network configurations.

Sentry Mode	Device Discovery
DM-SENTRY-NANO-BAC: BACnet/IP	The BACnet Sentry device will automatically discover the IP device behind it and contact the DIA for its provisioning information, including network keys, operational certificates, and firewall settings. For this automated discovery, the Sentry device requires the BACnet/IP device to respond to a Who-Is request with an I-Am response on every configured BACnet port.
DM-SENTRY-NANO-TCP: TCP/IP	The TCP/IP Sentry device may not automatically find the IP Address of the IP Device behind it. To manually enter the IP address the installer can connect the serial port and login to the user "config" and supply the IP Address of the device behind the Sentry device. The Sentry device will then probe that device and, if it's found, it will finish its configuration process.

Note: The Sentry device, by default, will use Multicast DNS (mDNS) to request network information from the DIA in order to fully come online. In situations where mDNS discovery does not work, the configuration process allows the installer to also supply the information that would be discovered automatically. This manual configuration of network parameters can happen prior to installation (whereas the IP address input for a TCP/IP Sentry device can only happen in real-time during deployment). Once you confirm your entries, the Sentry device will take these settings in lieu of discovering them from the DIA.

Sentry device commands are initiated by logging in from the command prompt with command-specific usernames and passwords as show in the table below.

Username	Password	Description
config	[none]	<u>For TCP/IP Mode only</u> The Sentry device will automatically configure parameters from the protected device if possible or prompt for manual configuration as follows: Veridify DOME Sentry Configuration. Device connected. Enter device IP Address (a.b.c.d): If the entered IP address is found, it will continue to the main menu (below); if not found the prompt for an IP address will be repeated. Entering a blank IP address will exit configuration. <u>For All Modes</u> After entering config mode, the following main configuration menu will appear: 1. (D)isplay Configuration 2. (E)dit Configuratiion 3. (C)lear Confirguration 4. (Q)uit Configurator [Selecting the number or corresponding first letter of each option will work] <u>2. Edit Configuration</u> 1. Network Configuration 2. BACnet Port Configuration * D. Display config Q. Quit Editor * menu option only available with a BACnet-capable Sentry device <u>2. Edit Configuration >> 1. Network Configuration</u> Enter the CIDR Size (0-31) [this is followed by Gateway Configuration] 1. Use the .1 address (e.g. x.y.z.1) 2. Use the .254 address (e.g. x.y.z.254) 3. Enter an explicit address (Note: may not work a priori) 4. No Gateway [after selection, there is a prompt for the DIA IP Address] Enter DIA IP Address (a.b.c.d): [this is followed by a display of configuration parameters and a confirmation prompt]

		2. Edit Configuration >> 2. BACnet Port Configuration Port Configuration: portA[-portB][,...] Enter Port Configuration: [after entry the prompt returns to the Edit Configuration menu] NOTE: The config mode only works for Sentry devices that are not already provisioned by the DIA. Attempting to run this command with a provisioned Sentry device will result in the following message: Sentry already configured. Reset Sentry to reconfigure.
reset	Reset	The Sentry device will clear all provisioning and reboot, probing for a new protected device. Any previously-configured manual configuration data is re-used for the probe; the reset will not clear out any manually configured data. To clear out manual configuration data, reset the Sentry device and then re-run the configuration option and use the "Clear Configuration" option."
showconfig	[none]	The Sentry device will display information including the software version, device UUID, current IP Address information, and the list of protected devices. After a few seconds the system will return to the login screen.
showlogs	[none]	The Sentry device will display the real-time logs of the device, starting from a dozen entries before you logged in. The logs will continue to display for as long as you remain logged in. To exit log-viewing mode, enter a Control-C character, and the system will return to the login screen.

3.6 Sentry Device Installation Validation

The Sentry device is designed to auto-configure itself, discovering the device connected behind it and bringing itself onto the network with minimal user intervention. Follow these steps to determine if the Sentry device was installed correctly and is operating properly.

Step 1: Connect the Sentry device and power it on as per the instructions, and watch the LEDs on the device. See the table in section 3.3 for the configuration states and LED indicators.

Step 2: Once the LED sequence becomes Flashing/On/On (or Flashing/Flashing/On) the device is operating normally. You will see the Sentry device as “online” in the DIA Device Inventory List, and the Sentry device will show up into the DOME Dashboard. The DOME Mobile App will also show the device as online and whether it is in Secure or Insecure (Pass-through) mode.

Step 3: Once the Sentry device is online in Secure mode (Flash/On/On), you can run Wireshark on the network to see the encrypted data.

Note - If the Sentry device does not reach the online state and stays in any other state for over 60 seconds, please see the Troubleshooting Guide.

3.7 Sentry Device Reconfiguration or Changing the Protected Device(s)

Sometimes end devices need to be replaced. Because the Sentry device is tied to the IP device behind it, if the protected device needs to be changed, the Sentry device will need to be reconfigured to allow that change by using the "reset" user account. Similarly, if the protected device is a BACnet/IP router and a device is added or removed behind the router, the Sentry device will need to be reconfigured to allow those devices to communicate.

When a Sentry device is reconfigured, it will not lose its name/mapping in the DOME Server. It will just obtain new security credentials locally, re-discover the IP device behind it, and if device is a BACnet Sentry device and the device is a BACnet router, it will find all the BACnet devices that the Sentry device is protecting.

If the IP address needed to be manually entered, it will need to be done again now. However, any manual network settings (CIDR, Router, DIA) will be saved across a reset.

3.8 Sentry Device Replacement or Relocation

When a Sentry device is replaced, or relocated to protect a different device, certain parameters need to be updated. There are two methods to force this update:
1. Power cycle the protected device.
2. Wait 15 minutes from the time the new Sentry device is connected to the network and protected device.

3.9 Sentry Device Troubleshooting

Issue	Remediation
No LEDs light up	The Sentry device does not have power. Check the connections, power sources, and ensure the power connection is connected securely to the Sentry device and the power supply source is turned on. Next, test whether the issue is the Sentry device or the power supply. Take the Sentry device and use the enclosed USB Cable and plug it into a standard USB Power supply. If the Sentry deivce lights up after a couple of seconds, the issue is the power supply. If the Sentry device does not light up, the unit may be defective. Contact KMC Controls support.
LEDs show SYS: Flash WAN: On LAN 1or 2: Off	The Sentry device is waiting for a link from the protected device. Ensure the Sentry device is plugged into the network and ensure the protected device is both plugged into the Sentry device and powered on. If this stage lasts for more than 15 seconds, the Sentry device may not be able to find the device, most likely because the device is quiet, has not emitted any data, and has not responded to any probes from the Sentry device. First ensure that the protected device is powered up and online. Check the LEDs on the Ethernet ports to ensure they are lighting up. Finally, try connecting to the Sentry device console and login as "config" to manually configure the IP Address.
LEDs show	The Sentry device is trying to determine the additional network parameters

Issue	Remediation
SYS: Flash WAN: Flash LAN 1 or 2: Off	for the protected device required for the Sentry device to come online. If this stage lasts more than 60 seconds, it means that the Sentry device cannot reach the DIA via mDNS, and that has not been pre-configured. Check that the DIA is reachable or connect to the Sentry device console as “config” and manually configure the parameters. This state can also occur if the network cables are swapped and the Sentry device heard and attached itself to a device on the network instead of the protected device. If this is the case, fix the cabling and then power-cycle the Sentry device.
LEDs show SYS: Flash WAN: Flash LAN 1or 2: Flash	This is an error condition, which means the Sentry device has failed to find valid network parameters. This condition occurs in the following cases: • The Sentry device reached the DIA via mDNS but the data returned did not include any network configuration data. Go to the DIA and ensure at least one OT Network is configured. • The Sentry device reached the DIA via mDNS, but the DIA did not return OT Network Configuration data that matched the IP Address the Sentry device discovered. Go to the DIA and ensure the proper OT networks are configured.
LEDs show SYS: Flash WAN: Off LAN 1 or 2: Flash	The Sentry device is trying to communicate to the DIA to obtain its provisioning data. If this state lasts for more than 60 seconds, there could be one of several reasons: • This is a BACnet Sentry device, and the protected device does not respond to a BACnet Who-Is command. There is no remedy to this situation except getting the device to respond to a Who-Is when the Sentry device asks, which is required by the BACnet standard. • The Sentry device cannot reach the DIA. There are several possible reasons: o The Network configuration is incorrect (incorrect CIDR setting for the network). o The Sentry device requires a default gateway, but none was configured. o The configured default gateway is incorrect. o There is a firewall rule preventing the Sentry device from reaching the DIA. o For all of these cases, check and correct the configuration. • The DIA refuses to provision the Sentry device because the Sentry device is not registered to this installation. Verify that this Sentry device is listed in the DIA’s Device Inventory. • This state could also occur if you manually configured the Sentry device (to bypass mDNS) but wired the Sentry device backwards (connecting cables to the wrong ports). If so, swap the cables and power-cycle the Sentry device. • To determine the cause of the issue, connect to the Sentry device console and login as “showlogs” to get more information about what is failing.

Issue	Remediation
LEDs show SYS: Flash WAN: On LAN 1 or 2: On	This means the Sentry device is online and successfully provisioned. It should be operating correctly. Check the DOME Mobile App and DOME Dashboard for additional status.
LEDs show SYS: Flash WAN: Flash LAN 1 or 2: On	This means the Sentry device is online and successfully provisioned into INSECURE (pass-through) mode. If should be operating correctly. You can Check in the DOME Mobile App and DOME Dashboard for additional status.
Cannot reach protected device management service (e.g. webui)	By design, the Sentry device will block access to the protected device from unauthentic sources. Reaching the device varies based on the type of Sentry device: • In the case of a TCP/IP Sentry device, the only way to reach the protected device is to use another Sentry device and become part of the secure enclave. • In the case of a BACnet Sentry device, a firewall rule can be configured to allow non-BACnet access to the protected device. Go to the DIA and ensure the Firewall setting in the Sentry Configuration Page is set to allow packets through. Then push the configuration down to the Sentry device to gain access.

4. DOME Network Requirements

This section provides the requirements for preparing a network for a DOME installation.

4.1 Multicast DNS (mDNS)

Sentry devices make an mDNS request on port 5353 to the Multicast DNS group, 224.0.0.251 as part of auto-configuration. The DIA needs to be able to hear and respond to it, and the Sentry device needs to receive the response. Note that the initial request is made from a source address of 0.0.0.0, and this packet needs to reach the DIA. The DIA will respond back to the multicast group.

Note that in environments where mDNS is known not to work, the Sentry device can be manually pre-configured with the information it would acquire from the DIA via mDNS.

4.2 Multicast Time

The DIA broadcasts NTP messages on the Multicast Time group, 224.0.1.1. All Sentry devices must be able to subscribe to the multicast group to hear those announcements. After the Sentry device gets online, it will reach out to the DIA via Unicast to set and maintain its time.

4.3 IP Addresses for Devices to be Protected

The device to be protected must have a static IP address as DHCP is not supported by Sentry devices. As part of the auto-discovery process, Sentry devices will discover and assume the IP and MAC address of the protected device.

4.4 802.1x

Sentry devices do not support 802.1x authentication. 802.1x must not be enabled on the target network.

4.5 BACnet Broadcast Management Device (BBMD)

DOME does not support the use of a BBMD on the OT network.

4.6 Ports and DOME Data Directionality

4.6.1 DIA to DOME Server

The DIA communicates to the DOME Server using multiple TCP and UDP ports at the following hostnames:

- dome.veridify.com
- domeserver.veridify.com
- log-server.securerf.com
- dp-log-server.securerf.com
- veridifystaging.securerf.com
- Various Ubuntu Update Servers
- ppa.launchpad.net
- swupdate.openvpn.net

All connections to the DOME Server are outbound-only, initiated by the DIA.

Port	Protocol	Comment
53		DNS
123		NTP
443	TCP	DOME
1194	TCP/UDP	DOME
6514	TCP	DOME
8443	TCP	DOME

4.6.2 DIA to Sentry Devices

Port	Protocol	Comment
22	TCP	SSH
123		NTP
4123		NTP

4.6.3 Sentry Devices to DIA

All Sentries in the Installation must be able to reach the DIA using the following ports:

Port	Protocol	Comment
123		NTP
4123		NTP
5353		mDNS
6514	TCP	DOME
9999	TCP	DOME

4.6.4 Sentry Device to Sentry Device

All Sentry devices in the installation must be able to reach the BMS.

BACNet

Port	Protocol	Comment
47808 (or as configured)	UDP	DOME

TCP/IP

Port	Protocol	Comment
9000	UDP	DOME

5. Technical Support

Please direct all technical support inquiries to info@kmccontrols.com, or by phone at 1.574.831.5250 or 877.444.5622. Secondarily, contact Veridify Security at support@veridify.com, or by phone at 1.203.227.3151 (Option 6).

We value your feedback! To help us improve this document, click here to take a 3-minute survey. Your input helps us make our documents clearer and more useful.