Verkada

Camera Setup Best Practices

Table of Contents

General Overview

Each Verkada camera is architected to automatically connect to the Verkada cloud via a secure bi-directional communication channel in order to:

1. Upload footage, archives, screenshots and thumbnails, plus alerts on certain event criteria (camera offline/online, Person of Interest, motion, tamper, crowds),
2. Download firmware and update settings from Command (such as optical zoom and security enhancements).

Verkada cameras do not connect to on-prem 3rd party NVRs and do not use insecure protocols (like HTTP or RTSP). If integration with SIEMs is required, this is always done via the Verkada cloud, as described in the **Alerts** (see page 12) section.

Installation and Setup

Powering and Connecting the Cameras

Verkada cameras leverage Power over Ethernet (PoE) for power and communication over your LAN. In most cases, cameras will connect directly to an access switch that supports the 802.3af PoE standard. If you are using an outdoor Verkada camera in a cold-weather climate and require the built-in heater, you will need a PoE injector or switch that supports the higher-power 802.3at PoE+ standard. The switchport must be configured as an access port, and all cameras will negotiate at full duplex (all models have 10/100Mbps NICs, with the exception of D80, which has 10/100/1000).

TIP

Always make sure the PoE budget on the switch is not exceeded. If it is, the camera will not power on or will be stuck with a constant Orange LED light.

If PoE is not available on your Ethernet switch, we recommend ordering additional PoE injectors and inserting them between the camera and the switch.

For existing deployments using coaxial cable, it might not be feasible to re-cable with Ethernet, and in that case, we recommend using converters as detailed below:
https://help.verkada.com/en/articles/3152569-powering-a-verkada-camera-over-coax

A few specific use cases are detailed in the following links:

Operating over LTE: https://help.verkada.com/en/articles/3062805-using-a-verkada-camera-on-a-cradlepoint-connection

Using wireless bridges: https://help.verkada.com/en/articles/3168378-connecting-a-verkada-camera-via-a-wireless-bridge-point-to-point-connection

Using fiber as a backhaul: https://help.verkada.com/en/articles/3558954-using-verkada-over-fiber

IP Addressing and Subnetting

When the cameras are powered on, they will use DHCP to ask for a local IP address. Currently, there is no support for static addressing, as this will entail connecting directly to the camera and setting it up, a behavior not allowed for security reasons. If there is a requirement to have fixed IP addresses, this can be done on the DHCP server using DHCP reservations, a process of matching a reserved IP address with a camera's MAC address. Verkada can provide a list of MAC addresses from a Sales Order upon request.

TIP

We strongly advise to separate cameras in their own VLAN, and use ACLs to limit inter-VLAN communication. This will add a layer of security, and will mitigate performance issues that arise when too many devices share the same broadcast domain. To support local streaming, you will need to configure the ACL to allow for bidirectional TCP 4100 (please see the Local Streaming/Offline Mode section for more information). Using VLANs will also allow you to adequately mark the traffic from a QoS perspective, to make sure it is prioritized in favor of bulk traffic (marking recommended: DSCP 40, CS5 - Broadcast Video).

The cameras work with existing 802.1x RADIUS infrastructure, and we recommend setting up MAC Based Authentication which uses the MAC address as opposed to username and password. All Verkada cameras start with a unique MAC OUI (Organizationally Unique Identifier) which starts with E0:A7:00. The full MAC address can be viewed by looking at the bottom of any Verkada camera when the mount is removed as well as on the Devices page.

Firewall Settings

Verkada cameras initiate communication to the Verkada cloud from within your network, so there is no need to set up any port forwarding. In addition, as the cloud is acting as the VMS, there is no need to utilize client VPN to connect to the LAN, if viewing footage remotely. However, the firewall between the LAN and the Internet needs to allow communication over HTTPS (TCP port 443) and NTP (UDP port 123). If either HTTPS or NTP are blocked, the camera will not boot properly. This will be indicated by the LED light on the camera being stuck on Orange, or flashing Blue.

TIP

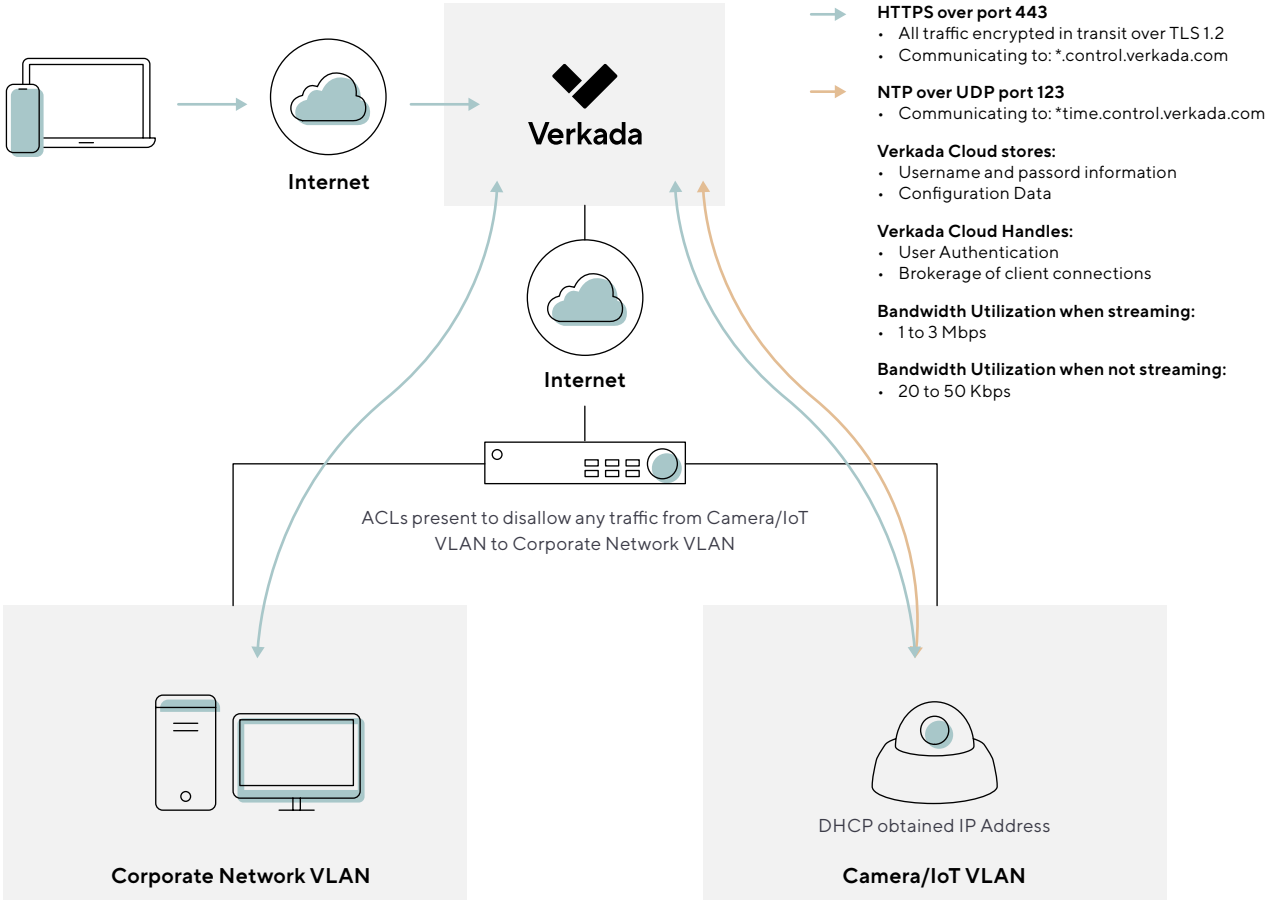
The easiest way to check if the ports are open, especially useful if the firewall is managed by a 3rd party, is to connect a laptop to the switchport, and:

1. Go to any HTTPS website (such as Google)
2. Verify NTP to 'time.control.verkada.com' (as seen below)

```
C:\Users\Luke>w32tm /stripchart /computer:time.control.verkada.com /dataonly /samples:5
Tracking time.control.verkada.com [216.239.35.0:123].
Collecting 5 samples.
The current time is 12/03/2021 08:54:22.
08:54:22, +00.2662246s
08:54:24, +00.2667521s
08:54:26, +00.2662741s
08:54:28, +00.2664762s
08:54:30, +00.2667384s
```

As best practice, we recommend setting specific rules whitelisting the Verkada domains used, as opposed to allowing all TCP 443 and UDP 123 traffic. A comprehensive list can be found at: https://help.verkada.com/en/articles/4132169-required-network-settings

Below, we have outlined expected VLAN separation and traffic flows:



All Verkada cameras use AWS PKI to ensure they only talk to the Verkada cloud, so SSL decryption needs to be turned off when inspecting Verkada traffic. Any attempt to enable it will break the communication. Examples bellow:

Zscaler: https://help.verkada.com/en/articles/4316383-using-zscaler-with-verkada

Palo Alto: https://help.verkada.com/en/articles/4048220-verkada-cameras-with-ssl-decryption

Bandwidth Considerations

Although the Verkada system utilizes just a small amount of bandwidth (typically 20-50 kbps at rest), we recommend that you review the current utilization of your ISP links in order to avoid scenarios where the cameras will be deployed in an already oversubscribed environment. This can lead to a wide range of issues, such as remote streaming not working properly or the camera having issues downloading firmware and maintaining proper operation.

Note that the cameras need to be able to route and reach the Verkada cloud, as described in the Firewall settings section, and will work no matter if you are using DIA (Direct Internet Access) or centralized breakout out of a remote main site (when using MPLS to connect). If the site has both direct Internet links but also MPLS, we recommend setting up routing policies to prefer the former and use the latter just as backup (if Internet breakout is possible).

When trying to compute the bandwidth requirements for a camera, you need to account for:

1. The bandwidth consumed at rest (when nobody is viewing footage); this tends to be between 20-50 kbps, and can go upwards to 100+ kbps with advanced analytics (face search, person/vehicle characteristics search) turned on, especially in a scene with a lot of activity.
2. The bandwidth needed when footage is viewed; this is around 600 kbps for SD, 1.5 Mbps for HD, and between 2 to 3 Mbps for 4K.

A few important things to consider:

- When multiple users watch the live feed remotely, only one stream will be generated as AWS will multiplex the video.
- When watching historical video, the bandwidth used will increase linearly with the playback speed (2x faster playback results in 2x increase in stream bandwidth).
- Cloud backup bandwidth is identical with the usual stream bandwidth if set up for constant upload.

Tips for conserving bandwidth, if required:

- Disable advanced analytics if not used (the camera will still identify people and vehicles, but things such as Person of Interest or searching by clothing or vehicle color will not be available).
- Use the Cloud Backup schedule to upload footage outside working hours (if Cloud Backup is required).
- Enable Local Streaming to allow for the cameras to stream directly to the local device.
- Default all stream viewing quality to SD from the Cameras section of the Admin tab (the users can still change it to HD if needed).

Local Streaming/Offline Mode

When the camera's live stream is accessed, the device accessing it prioritizes streaming over the LAN. If the private IP address of the camera is reachable from the computer, as well as the proper domains are allowed on the network, the computer will establish an HTTPS connection with the camera to directly get the live feed. This means that the camera does not need to upload the data to AWS just for it to come back to the same location. This ensures that the ISP bandwidth is not overutilized, and the delay is minimal.

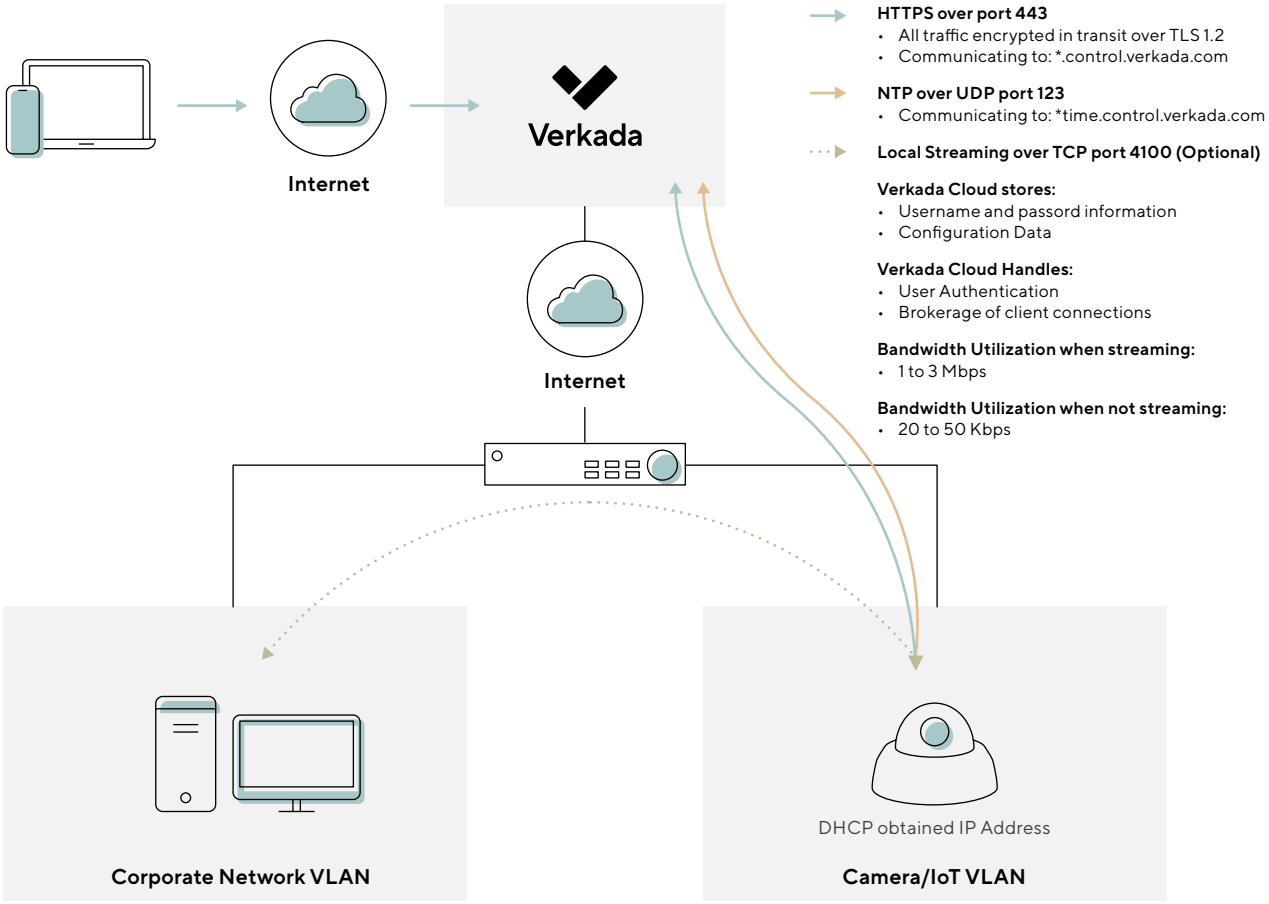
Requirements for **Local Streaming**:

- The accessing device must be able to reach the private IP of the camera.
- TCP Port 4100 needs to be open - bidirectionally between client and camera.
- No proxies between client and camera.
- Whitelist the domains found on: https://help.verkada.com/en/articles/3712294-local-stream-on-verkada-cameras

TIP
ACLs should be used to limit the traffic between the VLANs to TCP Port 4100.

You can determine if you are streaming live video directly from a camera if you see the following: the words "SD - LOCAL", "HD - LOCAL" or "4K - LOCAL" at the bottom left of the camera feed or a green dot with a white border around it next to the timestamp. If you only see "SD", "HD" or "4K" on the stream, then the video is being relayed through the Verkada Cloud.

Please note that whether a live stream is relayed through our servers or comes directly off a camera, security is equally maintained by using an encrypted TLS connection. See the diagram below to observe how traffic flows directly between the corporate device and the camera:



Offline Mode builds on top of Local Streaming, allowing live video to continue even in case of Internet outages. It will work if the device was already successfully logged into Command before the outage occurred, and the right certificates are installed (and trusted). A guide showing how to download and provision these certificates can be found on: https://help.verkada.com/en/articles/2937989-offline-mode-in-command

TIP

If you are looking to use Offline Mode at certain locations, we recommend testing it by momentarily disconnecting the ISP link. This should be done outside working hours, as per change management procedures. If successful, a banner will be displayed in Command, to notify you are in Offline Mode, and you will only be able to access live footage from the cameras that are still reachable from your end device.

When using Offline Mode, we recommend reserving an IP addresses through your DHCP server, as any address change while the ISP line is down will not be picked up by the cloud, and the viewing device will not be able to learn it has changed.

Time Synchronization

Verkada uses its own servers to sync the time on the cameras over UDP 123. Currently using your own NTP servers is not possible. If you wish to change the time zone setting of a particular camera, you will need to change its address (this can be done from the Info tab within any camera).

Firmware Updates

All Verkada firmware updates are delivered over-the-air (OTA). There is no action required from the admin in order to facilitate the firmware updates. When pushed, each camera will download the new firmware while continuing to operate, then reboot for a few seconds in order to apply it. To ensure failsafe updates, each Verkada camera is equipped with a dual-partition firmware bank. In the unusual event that a firmware update fails, the camera will automatically failover to the previous version of the firmware. In addition, a random variable is introduced in the process in order to make sure the cameras at a particular location do not all reboot at the same time.

TIP

You can check if the camera is up to date by going in the Device tab, clicking on it, and inspecting the Firmware section.

Configuring System Alerts

Each Command admin can subscribe to different types of alerts, such as:

1. **Camera Status:** the camera going offline or back online.
2. **Tamper:** triggered by the onboard accelerometer in case someone is trying to unscrew or is making contact with the camera.
3. **Motion:** can be configured to alert on general motion, or persons and/or vehicles in a certain area of the frame, either 24x7 or at a given time (via a schedule).
4. **Person of Interest:** when certain individuals are spotted across any camera inside the organization after their profile is flagged in the People tab.
5. **Crowd:** if more than a certain number of individuals is spotted in the frame at a given time.

Please note that motion and crowd notifications have to first be configured on a per camera basis to instruct the camera to push alerts into the Verkada cloud. If this is not set up, those cameras will not serve alerts. Each camera notifies on status and tampering by default, so it's just a matter of subscribing to the alert.

Currently the system uses SMS and email to provide the alerts. Furthermore, if the Verkada mobile app is installed on an Android/iOS device, Verkada will also send notifications natively (make sure you are logged in, and the OS is not blocking them). Read more on the setup on:

https://help.verkada.com/en/articles/3822777-notifications-page

If you are using a 3rd party system for ticketing/alerts, you can either use generic email addresses to direct emails to it, or utilize our extensive API and webhook capabilities, as outlined below:

https://www.verkada.com/integrations/

TIP

Make sure the email and phone number you use for your account are verified, if not no alerts will be received. In order to do that, click on the drop down arrow next to your name in the upper left side of Command, click the Profile tab, then make sure 'Verified is displayed next to your email and phone number.

Regarding **Camera Status** alerts, please be aware they do not signal necessarily that the camera is no longer functioning, but that the communication with the cloud has been interrupted for a significant amount of time. This can be triggered by things such as ISP outages, misconfigured firewall rules or even routing issues. If the camera is still powered, it will continue recording and offload relevant information and footage once the connection has been reestablished. If you want to get notified instantly that the camera, its cable, or the switch port they connect to has failed, please configure SNMP Traps on the switch (or other alarming mechanisms provided by the vendor).

User Identity

From Command, administrators can easily manage the users that have access to their organization. Below, we outline best practices and considerations for keeping your organization up-to-date and secure.

A robust approach to identity security is an essential component for managing access to the Command platform. There are two main approaches to consider for managing user access to Verkada Command:

1. Employing functionality native to the Command platform.
2. Leveraging an external identity provider, such as Azure AD or Okta.

External identity providers are purpose-built to provide your organization with a thorough approach to identity security. As such, we recommend using an external identity provider to benefit from the suite of controls they provide.

Controls for Identity Security

At a high level, there are a few different knobs we can turn to manage identity security in Command: how users access the platform, how users are added to the platform, and multi-factor authentication. For each of these controls, we contrast the Command-native approach to that of external identity providers.

Account Access

Native users within Verkada Command have a dedicated user account (username and password) that they use to access the platform. On account creation, the following password complexity requirements exist:

- Minimum of 8 characters
- At least one special character

Once created, native user accounts do not expire. As a result, we recommend ensuring that users follow existing organizational guidelines on password management.Using an external identity provider for account access, commonly called Single Sign-On (SSO), provides a number of benefits. The primary benefit of an SSO solution is that a single account can be used to log-in to any service supported by the identity provider. For example, the same account could be used to access Office 365 and their email.

Only needing to remember a single username and password reduces the chance of password reuse and password fatigue. SSOs also provide fine-grained controls over password length, age, and complexity, so these parameters can be in line with organizational policy. Additionally, Verkada Command allows organizations to enforce SSO-only login on their selected domains, so native user accounts cannot be used.

Verkada Command integrates with a number of SSO providers – in particular, SSO providers that support SAML 2.0. The list of providers can be found on Verkada's integrations page, with the designator SSO: https://www.verkada.com/integrations/. Additionally, we provide documentation on how to set up SSO for your Command organization through our supported providers: https://help.verkada.com/en/collections/2452528-verkada-command#saml-sso.

User Provisioning

Within a Verkada Command organization, native users are created in the users section **(Admin → Users → Add User)**. As we discussed previously, native users do not expire, so they must be manually removed if the account must be deprovisioned.

External identity providers that support SCIM provide a more robust solution: users can be automatically provisioned / deprovisioned through the identity provider, for all services that user has access to. In Verkada Command, this means externally managed users will be automatically created within Command when provisioned, and automatically deleted from Command when deprovisioned. Similarly, user groups can be managed by this same mechanism.

In either case, periodic audits of users within Verkada Command is highly recommended. It is important to be aware of who has access, and who no longer needs access (i.e. leaving the organization) so their access should be revoked. We highly recommend SCIM integrations if available, due to the ease of provisioning / deprovisioning and the consistency across multiple services. This approach greatly reduces the chances of a user having prolonged access and not being removed. The list of supported providers can be found on Verkada's integrations page, with the designator SCIM: https://www.verkada.com/integrations/.

Two Factor Authentication

Multi-Factor Authentication (MFA) provides additional login security beyond a username / password, by requiring other "factors" of security, e.g. an object the user physically possesses. Two-Factor Authentication (2FA) usually refers to the user entering their username/password (the first factor) and then requiring a code from the user's mobile device (the second factor) to complete the login.

Two-factor authentication is strongly recommended for all user accounts accessing Verkada Command. Two-factor authentication can be enabled natively in Command with the following steps:

1. Go to the top left of Command and click on your organization's name.
2. Select Profile under the Account section.
3. Click Enable for Two Factor Authentication.
4. Re-enter your account's password and follow the steps to finish configuration.

Command supports both SMS text and authenticator apps for mobile devices. If you are adding 2-factor for PCI compliance reasons, be sure to check the latest standards as mobile authenticator apps may be your preferred option. It is important to note: for native two factor authentication, there is currently no method to enforce 2FA on all accounts within your Command organization, as it is currently enabled by the user.

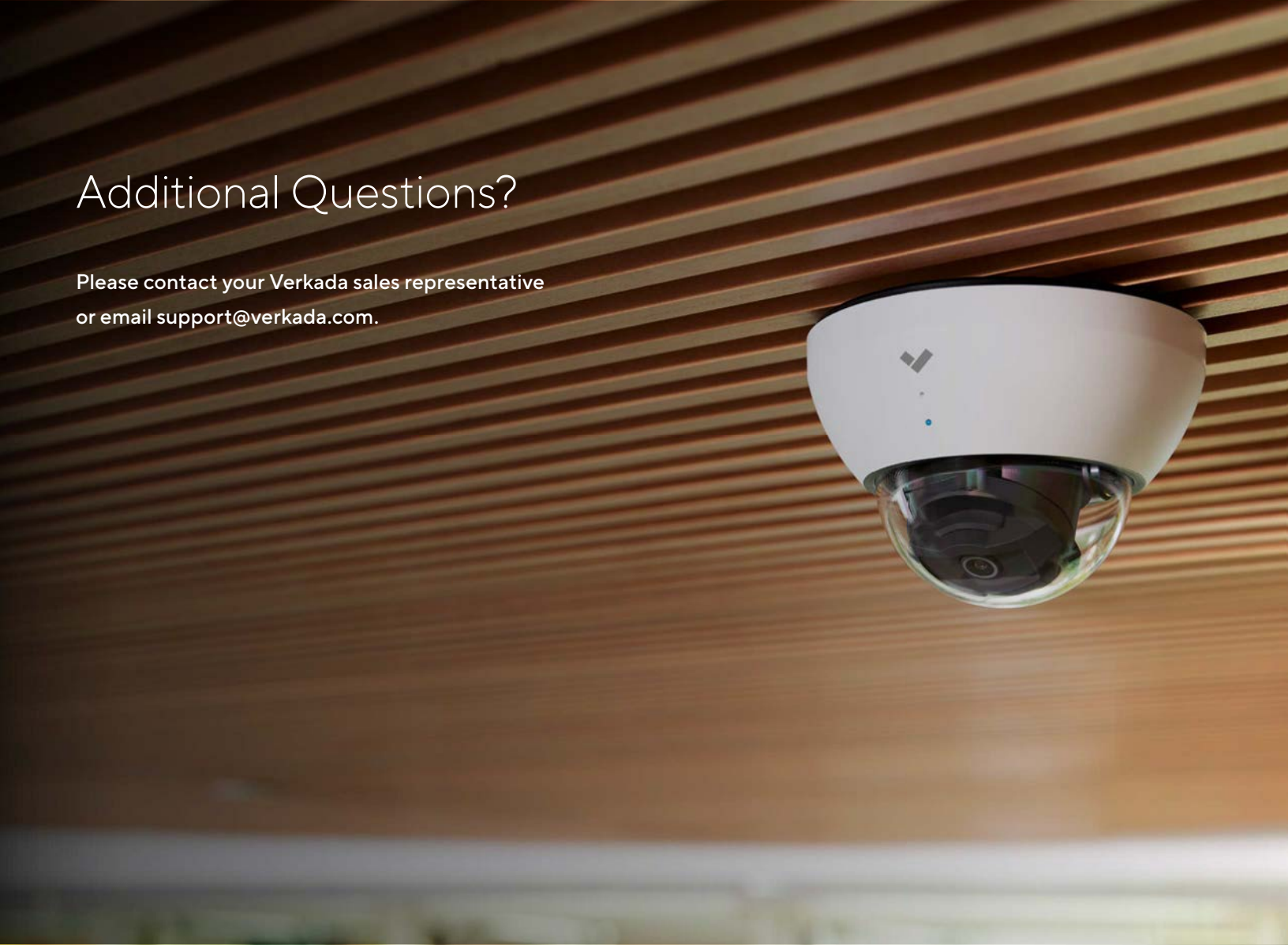
On the other hand, two-factor authentication can be enforced on all accounts managed through an SSO provider. For example, Azure AD allows the creation of conditional access policies which can enforce MFA for all logins.

Advanced Controls from External Identity Providers

Outside of the standard features listed above, a number of external identity providers offer advanced features that allow for more granular access policies. These advanced features often include restricting the login location based on the IP address, restricting a user to a particular device, and enforcing robust password requirements. We provide documentation on some of the more popular advanced features: https://help.verkada.com/en/articles/3858814-advanced-identity-security.

Additional Questions?

Please contact your Verkada sales representative or email support@verkada.com.



About Verkada

Verkada brings the ease of use that consumer security solutions provide to the levels of scale and protection that businesses and organizations require.

By building high-end hardware on an intuitive, cloud-based software platform, modern enterprises are able to run safer, smarter buildings across all of their locations.

USA HQ

405 E 4th Avenue
San Mateo, CA 94401, USA

Local: +1 (650) 514-2500

Toll-Free: 888-829-0668

General: sales@verkada.com

UK HQ

91-93 Great Eastern St Suite 3,
Hackney, London EC2A 3HZ, UK

Local: +44 (20) 3048-6050

Toll-Free: 0808-196-2600

General: sales@verkada.com