Verkada

Enterprise Controlled Encryption (ECE) FAQ

01. What is Enterprise Controlled Encryption (ECE)?

Verkada encrypts video data at rest (i.e., on the user's device or on Verkada's cloud servers) and in transit (i.e., as data moves among devices and the cloud). ECE builds on this encryption framework by giving organizations control over data encryption. Leveraging a well-recognized technique called client-side encryption, organizations can choose to keep some keys to themselves and share them with Verkada and third parties only if they want to, such as working with Verkada's technical support team. ECE improves on Verkada's already robust data protection measures–empowering organizations with control over their data.

02. How does ECE secure video data?

An Added Layer of Protection

With ECE, decryption requires access to two keys: one key is on Verkada servers, while the other is stored with the organization's identity provider (e.g., Okta, Microsoft Entra ID, etc.) Both keys are required to decrypt video, so even if there is a breach at the identity provider or Verkada, the other key helps keep the data secure. ECE is, in short, an additional security layer for data storage, combining the existing decryption step on Verkada's servers with a second step on the organization's own devices.

Customers Control Key Access

ECE puts decryption keys directly in the organization's hands–allowing one to selectively share access on an as-needed basis. This flexibility allows organizations to leverage the expertise of specialized services or comply with legal requirements while maintaining control over their data.[1] ECE allows organizations to decide who gets access to data, for how long, and to what extent.

03. How does ECE differ from Verkada's existing data protection measures? Why should an organization enable ECE?

Verkada has always prioritized data security with encryption both at rest and in transit. Data is protected, in other words, whether it's stored on a camera, on Verkada cloud servers, or when transmitted between the two. ECE adds yet another layer of protection by ensuring only authorized devices and users have the keys to decrypt data–giving organizations more control over who can access their data.

Let's illustrate the difference between encryption at rest and in transit and ECE with an analogy: imagine a retail store owner (the Verkada customer) uses an armored truck service (Verkada) to transport a bag of cash (video data) between the store (the Verkada camera) and a nearby bank (Verkada cloud servers). The cash is stored securely in the retail store's safe (data encryption at rest on camera), protected during transit in the armored truck (data encryption in transit), and once it arrives at the bank, it is secured in a vault (data encryption at rest in cloud).

Imagine now that the store owner places the cash in a secure lockbox inside the armored truck and only the store owner holds the key to this lockbox. Throughout the entire transit process—from the store to the bank—no one, not the armored truck driver, or the bank (Verkada), can access the contents of the lockbox because they don't have the lockbox key. Only the owner (the Verkada customer) has the key, and only the owner can access or decide who can access the content (video data).

04. Is ECE enabled by default?

No. Verkada cameras come with encryption at rest and in transit out-of-the-box. In order to take advantage of ECE, organizations need to enable it on Command.

05. How can organizations enable ECE?

Log in to Command and navigate to "Privacy & Security" under "Admin" settings. Click on "Enterprise Controlled Encryption" and complete all the steps. For more detailed instructions, refer to the Knowledge Base article.

06. Can I selectively enable ECE for specific devices, sites, or organizations?

Yes. As keys are generated on a per-device basis, organizations can enable ECE on one or all of their cameras. We recommend, however, that organizations enable ECE for all of their devices as it adds a significant layer of data protection.

1. Using ECE, an organization may wish to share its decryption keys with third parties for a number of reasons. An organization can allow a cybersecurity firm to conduct a safety audit to analyze video data without having permanent device access. During a time-sensitive investigation, an organization can additionally provide specific keys to law enforcement to grant access to relevant footage without exposing their entire video archive. An organization can, moreover, use a transcoding service to change the format of video or employ translation services and grant the service provider limited, task-specific access to data.

07. Can organizations selectively enable ECE for specific users?

No. ECE cannot be enabled for specific users in the organization as it works on a device level. If ECE is enabled on a device, it will apply to all users who have access to that device.

08. Why is Single Sign-On with OIDC required to enable ECE? Can Single Sign-On be used with SAML?

ECE decentralizes encryption keys used to secure data by giving control over one of the encryption keys to the organization. This key is generated on the organization's browser while an Org Admin is setting up ECE. Each user in the organization needs this key to successfully decrypt video and other encrypted data on Command.

To ensure all authorized users get access to this key, we rely on an identity provider (such as Okta, Microsoft Entra ID, etc.). The identity provider distributes this key to each user when they log in to Command, which is why Single Sign-On is required for ECE.

OIDC protocol allows organizations to add an attribute containing their encryption key while configuring Single Sign-On. This flexibility is not supported with the SAML protocol. In order to enable ECE, therefore, organizations need to configure Single Sign-On with OIDC.
We highly recommend moving from SAML to OIDC for Single Sign-On. OIDC is a more flexible and lightweight protocol that's easier to set up and manage.

09. Which identity providers are supported for Single Sign-On with OIDC?

As of October 2024, Verkada Command supports Okta and Microsoft Entra ID (formally Azure AD). To see an updated list of supported identity providers and the corresponding setup process, refer to our Knowledge Base article.

10. Are there any device, browser, or bandwidth requirements for ECE?

No. There are no additional device, browser, or bandwidth requirements for ECE.

11. How can I check if ECE is working after I enable it in my organization?

Once ECE has been successfully enabled, users will see an icon appear on top of the live and history player (next to the timestamp or camera name) within Command. See an example below:

For more information, refer to our Knowledge Base article.

12. What will happen if I lose my encryption key after enabling ECE?

Any data protected under ECE will become permanently inaccessible. It is of the **utmost importance** that users back up their encryption key.

13. What will happen if I enable ECE and do not log in via SSO OIDC?

If a user does not log in via SSO OIDC and they have ECE enabled devices, they will not be able to get their encryption key. This key is needed to decrypt video and other encrypted data. It means these users won't be able to access any footage on Command for ECE-enabled devices. We recommend either configuring SSO OIDC as "required" or always logging in via SSO OIDC. Note that SSO OIDC differs from SSO SAML and that ECE is not supported under SSO SAML. Organizations must ensure their SSO is set up in OIDC mode.

14. What will happen if I remove SSO OIDC configuration after ECE is enabled?

This is not recommended as users will be unable to access camera footage for ECE-enabled devices. If the user wants to remove SSO OIDC configuration, we recommend first opting out of ECE and then removing SSO OIDC configuration.

15. If I enable ECE, is Verkada completely prevented from accessing my video data?

No. In order to deliver certain analytics and features to organizations–particularly those features that require cloud processing–Verkada needs a temporary "unlock" to access a time range for a particular camera's customer footage. ECE still controls the access granted and Verkada does not gain unlimited access to customer encryption keys under ECE.

See the Knowledge Base article for a list of features that require necessary processing on Verkada cloud servers.

16. Are all camera features compatible with ECE?

It depends. Almost all camera features will be compatible (i.e., they will continue to work with ECE). This does not mean, however, that all data utilized for these features will be ECE-encrypted. RTSP streams will, for instance, continue to work once ECE is enabled but these streams are not encrypted by Verkada as they are meant to be ingested into third-party services outside of Verkada's platform. If Verkada were to encrypt these streams, these third-party services would not be able to decrypt them, which can pose an issue for our users.

To get an updated compatibility list of camera features with ECE, refer to our Knowledge Base article.

17. Which data is encrypted with ECE?

ECE applies to the original video data for each enabled device. ECE does not currently apply to image snapshots used to aid browsing and search experiences. To maintain interoperability with third-party systems, notably SMS and email providers for alerts, some configurations necessarily require sending some decryptable data to the cloud.

To get an updated list of configurations that necessitate decryptable data, refer to our Knowledge Base article.

18. Can I opt out of the features that require backend processing if I do not want Verkada to access any of my video data?

No. Organizations cannot explicitly opt out of every feature that requires backend processing, though they can opt out of certain features by navigating to the "Feature Manager" section under "Admin" settings in Command. This ensures organizations can take advantage of ECE's advanced data protection while minimizing any impact of their daily operations.

To get an updated list of camera features that require backend processing, refer to our Knowledge Base article.

19. Can I opt out of ECE?

Yes. Log in to Command and navigate to "Privacy & Security" under "Admin" settings. Go to "Enterprise Controlled Encryption" and click on "Remove."

For more detailed instructions, refer to our Knowledge Base article.

20. If I opt out of ECE, does it mean that my devices are unprotected?

No. All Verkada devices include encryption at rest and in transit by default. If an organization decides to opt out of ECE, their devices will revert back to the default encryption at rest and in transit–an industry standard.

Even though the default at rest and in transit encryption provides protection against many threats, we recommend organizations transition to ECE as it enhances data protection and security beyond the default encryption.

21. Does ECE apply to all Verkada product lines?

No. As of October 2024, ECE is only supported on Verkada's video security cameras.

For the latest information, refer to our Knowledge Base article.

22. How does enabling support access work with ECE?

Support access is fully compatible with ECE, allowing organizations to maintain encryption while granting Verkada support access. As usual, organizations can choose to include or exclude sharing video and image data. Access can be revoked at any time by the requester and automatically expires after a set duration.

From a technical perspective, the Support Access token is used in combination with linked ECE data as a password to derive the encryption key on the authorized Verkada personnel's web browser without having to send the key to the backend. The linked data along with the token expires together, preventing key derivation once the token has expired.

23. Which camera models support ECE?

For an updated list of supported devices, refer to our Knowledge Base article.

24. Does ECE disrupt the streaming experience on Command?

No. ECE is built to support the same high-performance technologies that Verkada has previously engineered for a non-ECE experience.

25. Is ECE available for non-Verkada cameras using Command Connector?

No. ECE only applies to Verkada cameras.

26. Are there additional protections in place if an unauthorized third party were to access the encryption key in my identity provider?

Yes. The secret value placed by the user in the identity provider does not directly encrypt the data. A logged-in account is required to turn the encryption key in the identity provider's metadata into the actual encryption key.