Frequently Asked Questions for Microsoft Entra Verified ID

Microsoft Entra Verified ID

What is Microsoft Entra Verified ID?

Microsoft Entra Verified ID is a managed verifiable credential service that lets organizations build unique user-owned identity scenarios designed for trustworthy, secure, and efficient interactions between people and organizations.

How does Microsoft Entra Verified ID work?

Microsoft Entra Verified ID uses verifiable credentials as a secure way to digitally prove someone's identity, qualifications, or any unique identity attributes. Users own their Verified ID credentials and store them in a digital wallet. When asked to prove their identity, they can present their credentials to a verifier.

Why should my organization use Microsoft Entra Verified ID?

Microsoft Entra Verified ID enables your organization to build unique solutions that address their specific identity-related issues, provide quick, transparent, and more secure verification for customers and employees while reducing costs, risks, and business inefficiencies associated with managing user identities.

What are common scenarios in which Microsoft Entra Verified ID can help my organization?

- **Help desk & account recovery**: provide a quick and secure remote self-service help desk for your users to recover their account, change their password, or other complete other help desk activities
- **Remote onboarding**: quickly verify the identity of new employees or external users through self-service enrollment
- **Access package in entitlement management**: As an access package manager, you can require that requestors present a Verified ID containing credentials from a trusted issuer such as a training certification, work authorization, or citizenship status

How can I get started with Microsoft Entra Verified ID?

Microsoft Entra Verified ID is included for free in Microsoft Entra ID P1. Check out this quick setup tutorial to start using Verified ID.

Is Microsoft Entra Verified ID based on open standards?

Yes, open standards are guidelines made available to the public that facilitate interoperability among different decentralized identity products such as verifiable credentials. Microsoft pioneered development of decentralized identity standards as an active member of the Decentralized Identity Foundation (DIF) and World Wide Web Consortium (W3C), two leading decentralized identity open standards organizations. Microsoft collaborates with the wider identity community to create these open standards and incorporates them into Verified ID to ensure that it works universally.

Learn more about open standards.

Does Microsoft Entra Verified ID use Blockchain technologies?

No, Microsoft Entra Verified ID uses verifiable credentials that are cryptographically secure for instant identity verification based on W3C DID standards.

Can a user back up a Microsoft Entra Verified ID credential?

Normally, it is easy to reissue a credential to your device. If a user wants a backup, they can export a credential from their Verified ID wallet on the Microsoft Authenticator application to a wallet on another device.

Can a Microsoft Entra Verified ID credential be stolen? What protections are in place to prevent usage of a stolen credential?

When exporting a credential to another device, a randomized 11-word passphrase is shown to the user. When importing the credential to the new device, the user must enter this passphrase to access the credential. If a credential was stolen, a Face Check verification would prevent it from being used by anyone other than the rightful credential holder. The original issuer can also revoke a credential if it is stolen. Revoking credentials is a normal action that occurs for several reasons, normally due to a user no longer needing it, such as an employee leaving a company.

Learn more about revoking a credential.

Face Check with Microsoft Entra Verified ID

What is the difference between Microsoft Entra Verified ID and Face Check with Microsoft Entra Verified ID?

Microsoft Entra Verified ID is a managed verifiable credential service that lets organizations build unique user-owned identity scenarios through a network of identity credential issuers, verifiers, and presenters.

Face Check with Microsoft Entra Verified ID is a premium feature within Verified ID used for privacy-respecting facial matching. It allows enterprises to perform high-assurance verifications securely, simply, and at scale. Face Check adds a critical layer of trust by performing facial matching between a user's real-time selfie and a photo. The facial matching is powered by Azure AI services.

Why would I want to use Face Check with Microsoft Entra Verified ID? Is Verified ID not enough for identity verification by itself?

Verified ID is effective for quick and secure identity verification. Face Check adds a different layer of trust and identity verification by evaluating a user's "liveness", which ensures that the right user is using a Verified ID credential in the moment it is used. If your organization wants to not only verify someone's identity but also check their liveness, consider adding Face Check to your application.

For many common identity verification tasks, Verified ID is enough. If an action is higher risk, an organization may want the layer of assurance that Face Check provides. For example, if an employee wanted to execute a basic help desk function, verifying their identity with their Verified ID is likely sufficient for the organization. If the employee wanted to reset their password or recover their account, this action carries a higher impersonation risk than others, so an organization may want to use Face Check to ensure in real time that the right person is resetting the account. Organizations can decide if they want to use Face Check based on the level of identity assurance they want for the risk of the action in question.

How can I start using Face Check with Microsoft Entra Verified ID?

To start using Face Check, the first step is to set up your Verified ID tenant. Then, set up Face Check and add it to your Verified ID service in minutes. There are two options to purchase Face Check and start verifying:

1. Begin the Entra Suite free trial, which includes 8 Face Check verifications per user per month.
2. Enable Face Check as a consumptive add-on within Verified ID and pay $0.25 per verification.

Visit the Microsoft Entra pricing page for more pricing details and updates.

How does Face Check with Microsoft Entra Verified ID work?

Face Check compares a person's real-time selfie with their photo previously uploaded to the Verified ID credential that an organization wants to verify. The Verified ID photo is usually from a trusted identity document, such as a driver's license or employee ID. Face Check's advanced algorithms will compare the two images to verify that both faces match and give a confidence match score to the verifying organization. In this process, the photos and sensitive data are not stored or passed to the verifier, and the confidence score is the only result shared from this process.

How high should my confidence score be?

Organizations can choose their confidence score threshold for their application to accept a Face Check verification. A higher threshold means that it is less likely for an impersonator to be falsely accepted. At the default and recommended confidence score of 70%, the chance that the person in the live selfie is not the rightful credential owner is one in 10 million. At a 90% confidence score, that chance is one in one billion. A higher confidence score threshold results in the increased potential for an authorized user being rejected due to the application's higher sensitivity. It is important to find the right balance between setting a high confidence score threshold that secures your application while not making it so high that it often rejects authorized users due to slight changes in appearance or the visual conditions of their surroundings such as lighting.

Learn more about facial matching and how confidence scores work

Can someone bypass Face Check with Microsoft Entra Verified ID with a picture or video of a credential holder?

No, Face Check is powered by Azure AI Vision Face API which is resistant to various spoofing techniques including using pictures, videos, or deepfakes of a user.

Face Check with Microsoft Entra Verified ID uses Azure AI Vision Face API liveness check to verify that it is a real person in the selfie footage from the camera on the user's device. This check helps ensure that a static photo or a 2D video of a user cannot be used in place of that user's live self.

Learn more about Azure AI Vision Face API

How fair is Azure AI Vision Face API?

Microsoft has conducted fairness testing of the Face API. The Azure AI services team is continuously striving to ensure responsible and inclusive use of AI.

View the Face API Fairness report

If a user recently got a haircut, shaved their facial hair, or otherwise changed their physical appearance, will they be able to complete a Face Check verification?

Face Check compares a user's live selfie to the photo associated with your Verified ID credential. The less the user looks like that photo, the lower their confidence match score will be. Whether the Face Check verification is accepted or not will depend on how differently the user currently appears from their previously saved Verified ID photo and how high of a confidence score threshold the application has. If your application has a relatively high threshold, it is recommended that users keep a physical appearance that is consistent with their uploaded Verified ID photo or replace the photo with one that reflects the user's current appearance.

Once I use Face Check, where does my data go? Where is it stored?

During a Face Check request, a selfie is captured from the user's mobile device. This image is passed to Verified ID which uses it to invoke Azure AI Vision Face API services, which compares the selfie footage to the Verified ID photo. Once done processing, the selfie image is discarded and not saved on any device or service. Microsoft Authenticator, Verified ID, and Azure AI services will NOT store or keep this data. Furthermore, the captured selfie image is not shared with the verifier application. The verifier application only receives a confidence score of the resulting match.

Learn about data and privacy for Azure AI services

What is the difference between Face Check with Microsoft Entra Verified ID and Multi-Factor Authentication (MFA)?

MFA is a strong authentication method that blocks 99.9% of account compromise attacks. Authentication ensures that someone has the right credential to access something and protects against unauthorized access. Someone could have the right credential and be "authenticated" to access a resource, but there is not a guarantee that the right person is using that credential.

Face Check with Microsoft Entra Verified ID verifies the identity of someone in a digital transaction with real-time facial matching. By doing a liveness check, Face Check ensures that the right person is using the right credential. Someone who completes both an MFA and Face Check is both authenticated and verified. MFA and Face Check complement each other by providing two different security layers.

What is the difference between Face Check with Microsoft Entra Verified ID and Windows Hello for Business?

Windows Hello for Business is an authentication technology that allows users to sign in to their Windows devices using biometric data, or a PIN, instead of a traditional password. It provides enhanced security through phish-resistant two-factor authentication, and built-in brute force protection. A Windows Hello profile is bound to a particular device.

Face Check is a high-assurance identity verification method that compares someone's liveness to a picture from a trusted identity document such as a drivers' license or passport. Face Check is designed for higher sensitivity scenarios such as verifying someone's identity before recovering their account or onboarding them into your organization. Verified ID is portable and not device bound. A verification could be done against any Verified ID credential in a user's wallet, and the verifying organization determines which credential to request for verification. The device someone is using does not determine which credential will be requested.

How is Face Check with Microsoft Entra Verified ID different from when I use my face to unlock my phone or access an app?

Both Face Check and the face-scanning security feature you may use to unlock your device require a user to face a camera, but they operate in different ways. Face Check compares the liveness data (selfie) with a photo from a trusted identity document, such as a driver's license or employee ID. This mechanism provides a crucial layer of trust, especially in high-assurance scenarios such as accessing high-value business processes or sensitive company information. The face-scanning feature on your device may compare your live face to a representation of your face stored on the device.

Does the Face Check with Microsoft Entra Verified ID verification happen in the wallet, or on the cloud?

The Verified ID service executes the verification process in the cloud, not on the device. Credentials are stored on a user's device so that they have full control of a credential's usage. A user must choose to share a credential with a verifier for it to be processed for verification.

Developer FAQs

Does Face Check with Microsoft Entra Verified ID require Microsoft Authenticator?

Face Check is limited to Verified ID usage with MS Authenticator. This limitation is in place to prevent an injection attack on Face Check.

What is the confidence percentage match and what does confidence % mean?

Face Check uses the same default confidence matching threshold as Windows Hello for Business. Developers can adjust it up or down depending on their specific usage scenario. The higher the confidence score, the more likely the match result is not a false positive.

Is iBeta Level 2 conformant?

Yes. Azure Face API AI and Face Check are iBeta Level 2 conformant to be resistant to various presentation styles of attack to impersonate a user.

Learn more about iBeta's ISO Presentation Attack Detection testing

What are the requirements for the photo in the Verified ID?

The photo should be clear and sharp in quality and no smaller than 200 pixels x 200 pixels. The face should be centered within the image and unobstructed from view.

Learn more about how facial points are detected in the image

Where can developers go for more resources?

To learn more about Microsoft Entra Verified ID, see demos, follow tutorials, read articles, or see code samples, visit the Verified ID Developer Page.