Verifying your devices is becoming mandatory

November 19, 2025 SECURITY

Act now: continue sending & receiving encrypted messages

In April 2026, we will be rolling out a significant update to strengthen the security of your conversations: unverified devices will no longer be able to send and receive end-to-end encrypted messages via Element. This change follows the Matrix **specification update** that was announced at the Matrix 2025 conference on October 17 and benefits everyone by

This security update will give you assurance that when you receive a message from a contact, you can effortlessly assume it's really from them.

It's a big step towards making Element an even more safe and reliable messaging experience. We mean it when we say that we want to provide the most secure communication technology in the world.

So here's what's changing and why it matters to you.

Unverified devices are a potential attack vector

Imagine you're messaging a colleague and suddenly a warning shield icon appears on your screen. Is this just a harmless unverified device and you can safely ignore the warning, or has someone's account been compromised? At best this is a distraction and, at worst, it is someone malicious trying to impersonate one of your contacts - neither is ideal. What's worse is that ignoring these warnings leaves unmitigated risks to proliferate throughout your network.

With Element, trust is critical - a non-negotiable. For example, we provide end-to-end encryption by default to all of our users to ensure that you and the person you're messaging - and only the person you're messaging - can read the messages. This forthcoming change aims to eliminate uncertainty and the likelihood of malicious activity by requiring all devices to be verified.

Device verification matters

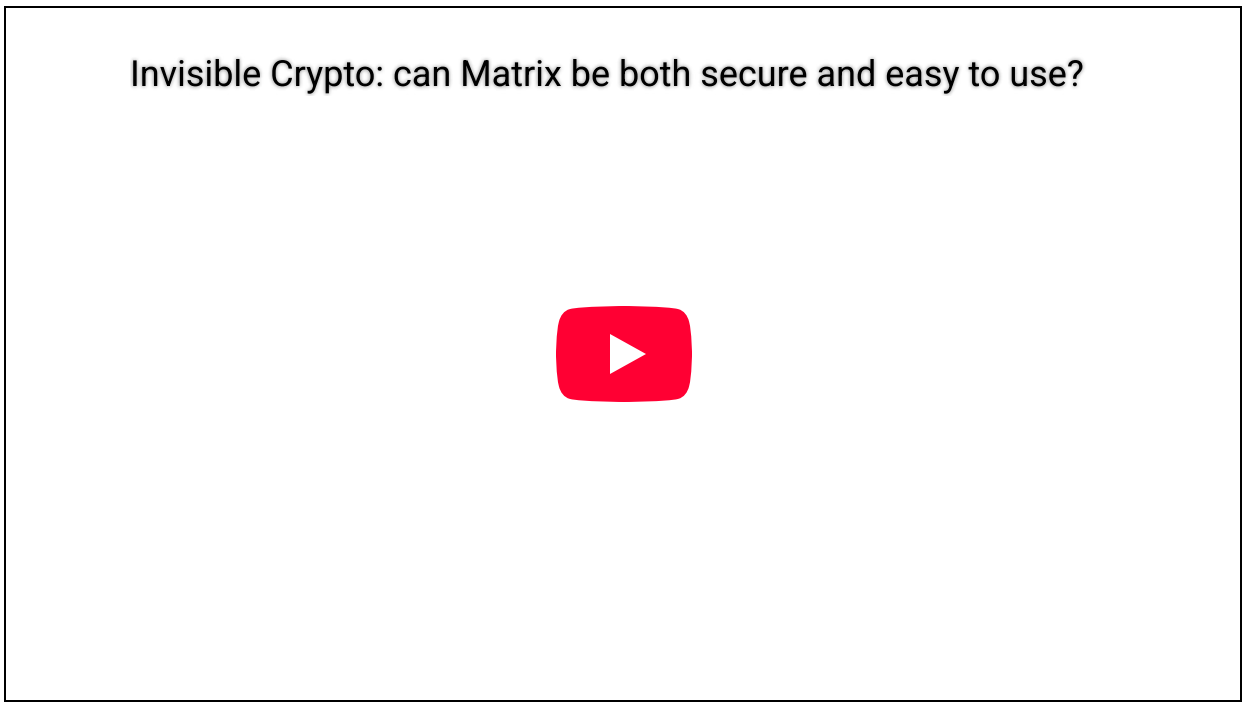
Device verification acts like a hand shake between your devices, proving cryptographically to your contacts that they belong to you. Without this

Trust by design and default

Going forward devices will be either verified or unable to participate in conversations - it's that simple. No more warning or shield icons that can be easily ignored, these ultimately undermine the impact of important warnings/notifications (users become desensitised).

By verifying your devices, you're not just protecting your own communications, you're creating a more trusted environment for everyone.

We're designing a system that prioritises the security of your communications and making verification an integral part of the process is a great example of that.



Action required by end users

If you're already in the habit of verifying your devices and have your recovery key set up there's nothing you need to do to prepare, you're good to go.

- Set up recovery if you haven't done that already.

Note: although setting up recovery is strictly not mandatory, it is highly recommended, as it simplifies the verification of new devices, and enables you to do that even when you lose all of your current devices.

For the details of how to do this on various platforms, please read more in the **user documentation**.

What if you don't verify...?

From April 2026:

- Unverified devices will no longer be able to send messages.
- Content of the messages received from unverified devices will not be shown (you can still see that there was a message).

In short, unverified devices will effectively become unusable in end-to-end encrypted (E2EE) conversations. You'll still be able to participate in conversations where E2EE has been deactivated, but in all other circumstances you will be excluded.

Building trust together

As stated above, trust is fundamental to secure communication. By requiring verified devices, we are raising the bar for what users can expect from your secure communication. This is a small change that makes a big difference. We have to work together with our users to ensure success. We're doing this work to ensure every message you send and receive is as trustworthy as a face-to-face conversation.

We're here to make the transition as smooth as possible. If you have questions or need help, our support team is ready to assist. Together

Andreas Sisask

Related Posts

SECURITY

Coordinated Matrix security update

A new coordinated security fix for all Matrix server

Element Secu... 11/08/2025

SECURITY

End-to-end encryption

Many vendors claim to offer end-to-end encryption. Most

Patrick Alberts 27/05/2025

GOVERNMENT

How Element protects against Signalgate style accidental invites

Element Server Suite enables

Steve Loynes 3/04/2025

SECURITY

Running outdated versions of Synapse is a problem

If you're still using the old

Archie W 20/02/2025

Element X and Pro updates; a glimpse into the future

At The Matrix Conference 2025

Andreas Sisask 12/11/2025

Element is the fast, simple and private way to communicate with family, friends, teams, colleagues, organisations and the wider world.

Thanks for reading our blog— if you got this far, you should head to **element.io** to learn more!

Get started