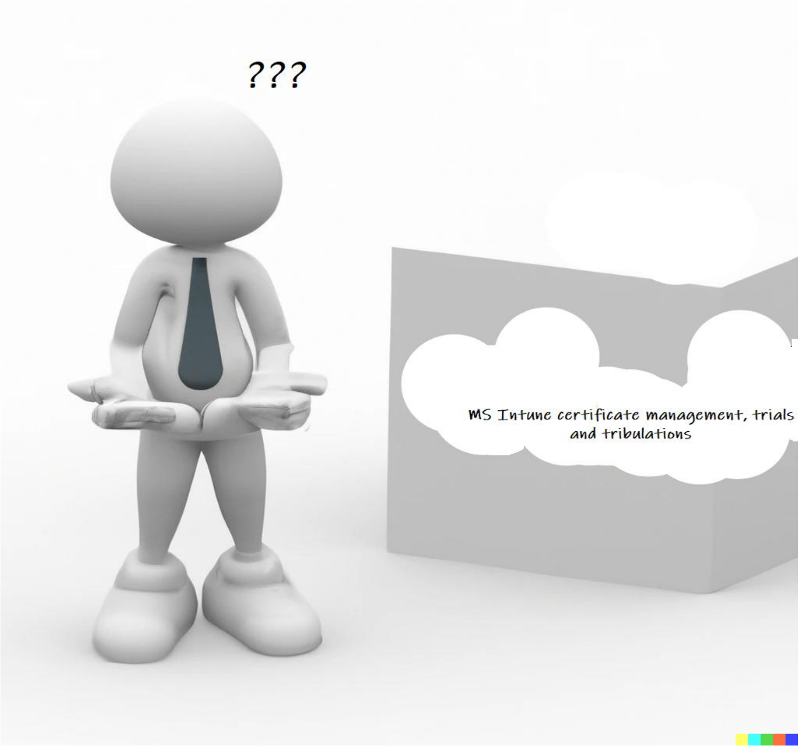
Whitepaper

So you want to know about deploying certificates using MS Intune, but don't know where to start?



Contents

The Challenge

I had read about it on Reddit and other online forums, but never thought it would happen to me – until I got a call from my CEO. "We've decided to start using Intune, and you've been designated as the in-house Intune specialist. Go forth with my blessing and make the magic happen."

Most of us actually know what Intune is – it's a mobile device management solution. I had read about it and heard others use it, but how does it actually work? Where should I start?

I figured, given our company's specialty, let's start with something seemingly easy – something I know a great deal about, and something that's supposedly easy with Intune but hard without MDM. Let's start with Intune-based certificate management for mobile devices.

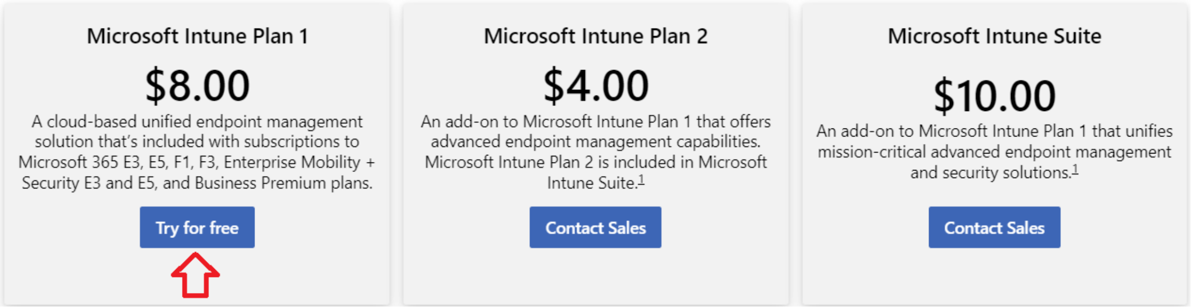
The Journey

Baby steps understanding Intune and first errors

First thing I did... go to the Microsoft website and read all I could on Intune.
https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Check, silly me, of course we need Intune licenses first.
So heading over to the Microsoft license ordering:
https://www.microsoft.com/en-us/security/business/microsoft-intune-pricing?rtc=1

Microsoft has a multiple Intune plans to choose from;



Microsoft Intune Plan 1

$8.00

A cloud-based unified endpoint management solution that's included with subscriptions to Microsoft 365 E3, E5, F1, F3, Enterprise Mobility + Security E3 and E5, and Business Premium plans.

Microsoft Intune Plan 2

$4.00

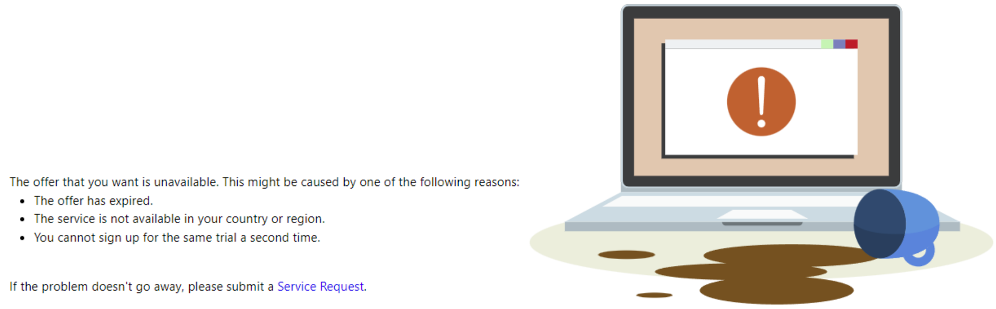
An add-on to Microsoft Intune Plan 1 that offers advanced endpoint management capabilities. Microsoft Intune Plan 2 is included in Microsoft Intune Suite.[1]

Microsoft Intune Suite

$10.00

An add-on to Microsoft Intune Plan 1 that unifies mission-critical advanced endpoint management and security solutions.[1]

The 'Try for free" option is interesting but… it doesn't work ☹

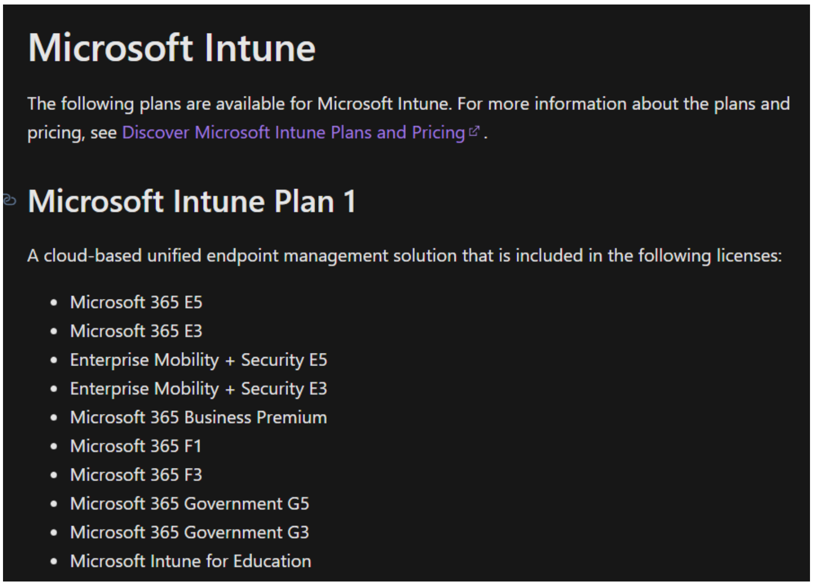


The offer that you want is unavailable. This might be caused by one of the following reasons:

- The offer has expired.
- The service is not available in your country or region.
- You cannot sign up for the same trial a second time.

If the problem doesn't go away, please submit a Service Request.

So now what? There's different license options for sure, and thankfully there are;



Microsoft Intune

The following plans are available for Microsoft Intune. For more information about the plans and pricing, see Discover Microsoft Intune Plans and Pricing.

Microsoft Intune Plan 1

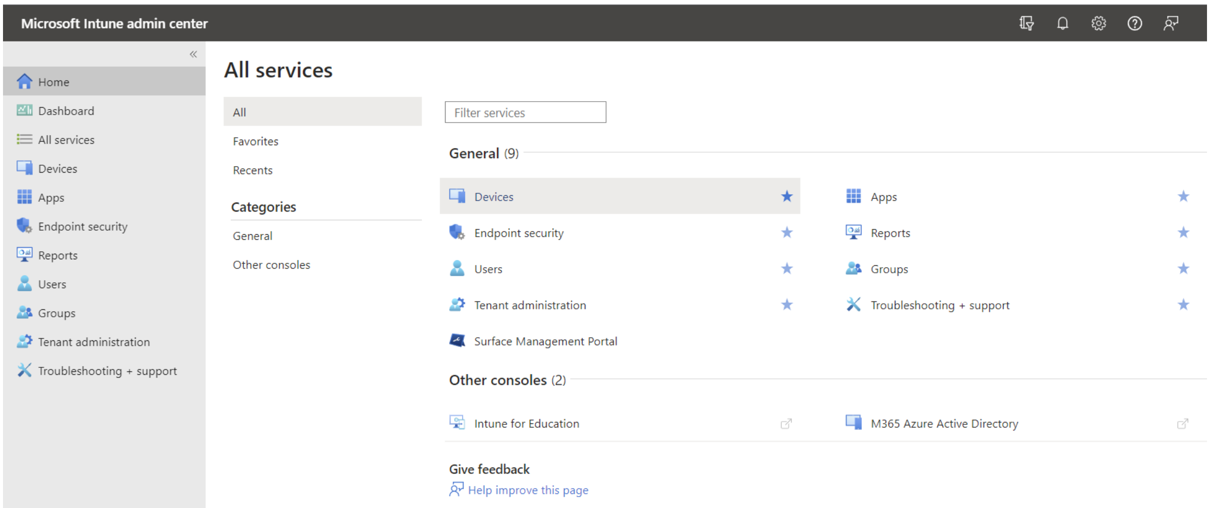
A cloud-based unified endpoint management solution that is included in the following licenses:

- Microsoft 365 E5
- Microsoft 365 E3
- Enterprise Mobility + Security E5
- Enterprise Mobility + Security E3
- Microsoft 365 Business Premium
- Microsoft 365 F1
- Microsoft 365 F3
- Microsoft 365 Government G5
- Microsoft 365 Government G3
- Microsoft Intune for Education

But where to start within Intune?

Google has the answers to everything, even when it comes to Microsoft products. Thankfully, there are plenty of resources available to learn about Intune. However, I realize that this will take up a lot of my time. I found some helpful tutorial videos on YouTube at this link: https://www.youtube.com/results?search_query=intune+mdm+mobile+device

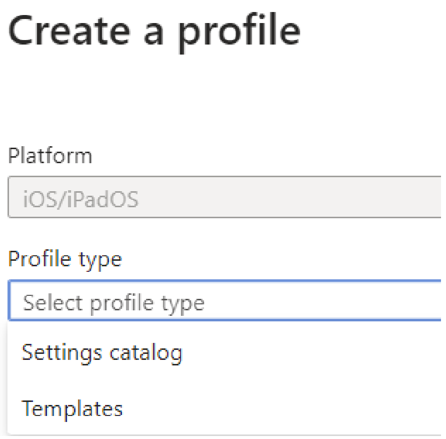
Learning how to navigate the interface was a bit of a challenge, but after spending a few hours clicking on different items and watching tutorial videos, it started to feel intuitive.



First Intune configuration, the waiting game starts

Everything in Intune requires a specific policy to be configured, per target Operating System, and for Android, per type of device control. So, every app installation, app configuration, and OS setting configuration needs to have a policy defined.

Since I want to start with deploying S/MIME certificates, it seems obvious to start with a device configuration profile, and since I have an iOS device, its easiest to start with iOS.



Create a profile

Platform

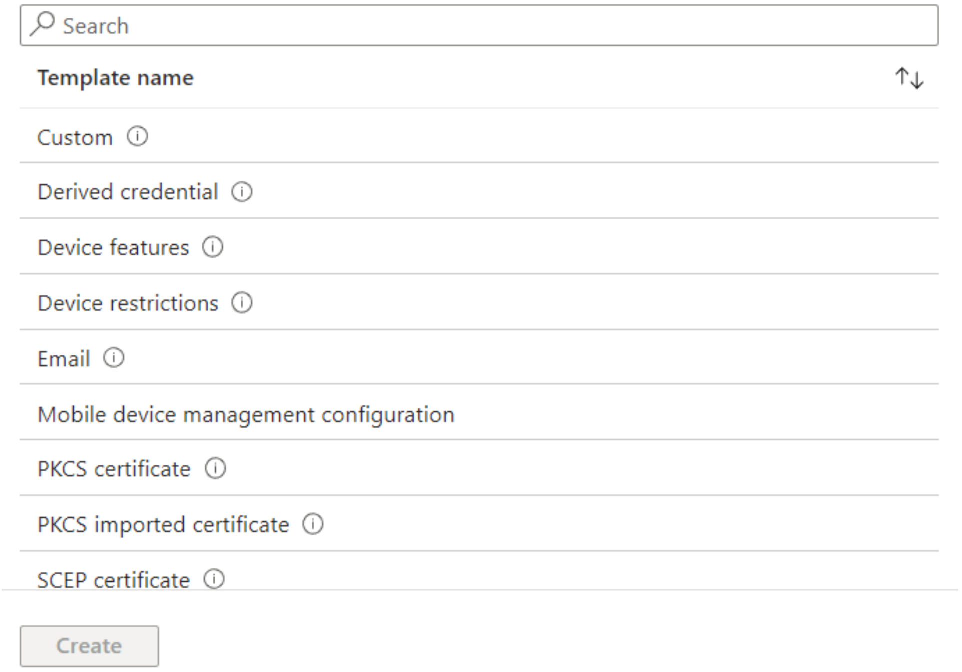
iOS/iPadOS

Profile type

Select profile type

More clicking seems required, as I have no clue yet how Settings Catalog differs from Templates, but hey 2 choices, so 50% chance I choose correctly.

Ok I chose wrong, but two times a charm and I can choose again:



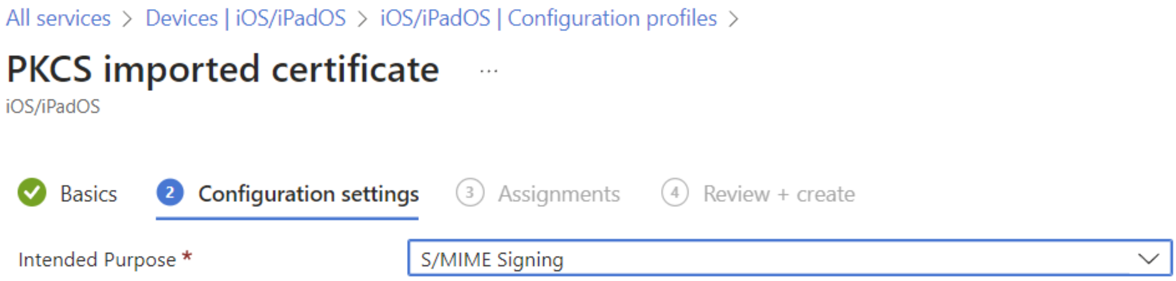
Template name ↑↓
Custom ⓘ
Derived credential ⓘ
Device features ⓘ
Device restrictions ⓘ
Email ⓘ
Mobile device management configuration
PKCS certificate ⓘ
PKCS imported certificate ⓘ
SCEP certificate ⓘ

So there’s 3 types of certificates I can deploy, but what’s the difference?

After reading Microsoft's article again, it quickly shows that Imported PKCS is needed, where imported PKCS stands for public key pair (PKCS) certificates https://learn.microsoft.com/en-us/mem/intune/protect/certificates-imported-pfx-configure

And what I've seen in Outlook for Mobile, I need to separately configure a signing certificate and an encryption certificate.

So my first policy will be S/MIME signing:

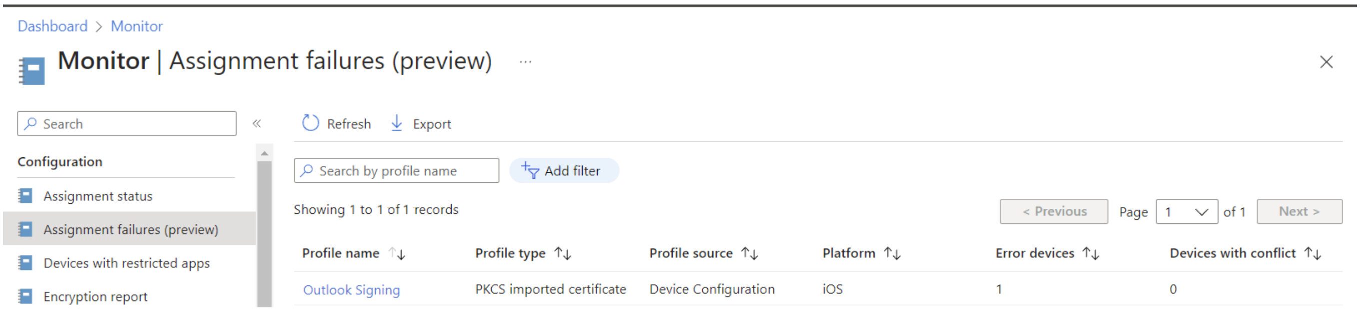

All services > Devices | iOS/iPadOS > iOS/iPadOS | Configuration profiles >
Basics
2 Configuration settings
3 Assignments
4 Review + create

PKCS imported certificate ...

iOS/iPadOS

Intended Purpose * S/MIME Signing

I save it, enable control of my iPhone using Intune and …… nothing happens nothing shows…. for over an hour, and then all of a sudden… did something actually happen?



Monitor | Assignment failures (preview) ...

Showing 1 to 1 of 1 records

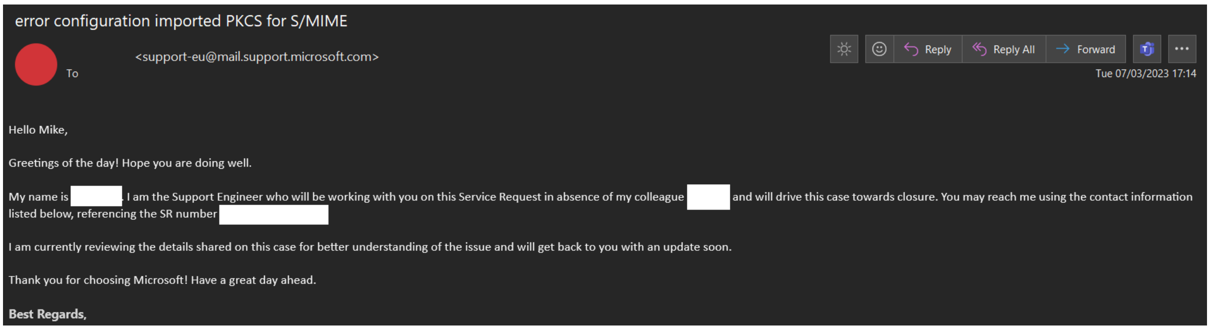
Profile name	Profile type	Profile source	Platform	Error devices	Devices with conflict
Outlook Signing	PKCS imported certificate	Device Configuration	iOS	1	0

Apparently regretfully not. Intune simply took a long time to display the error.

And since the error is not self-explanatory in Intune, its best to contact Microsoft support to ask what's going wrong.

Trouble shooting without and with Microsoft support

First of all, kudos to Microsoft Support for being so patient. I can't blame them for not knowing everything and taking their time to get advice from colleagues and other departments, especially in a field that seems underused. It takes a lot of time and patience (see time stamps), but they do persist and get things solved.


error configuration imported PKCS for S/MIME

<support-eu@mail.support.microsoft.com>

To

Tue 07/03/2023 17:14

Hello Mike,

Greetings of the day! Hope you are doing well.

My name is [redacted] I am the Support Engineer who will be working with you on this Service Request in absence of my colleague [redacted] and will drive this case towards closure. You may reach me using the contact information listed below, referencing the SR number [redacted]

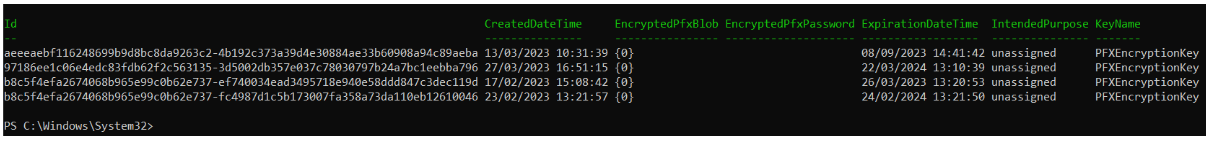
I am currently reviewing the details shared on this case for better understanding of the issue and will get back to you with an update soon.

Thank you for choosing Microsoft! Have a great day ahead.

Best Regards,

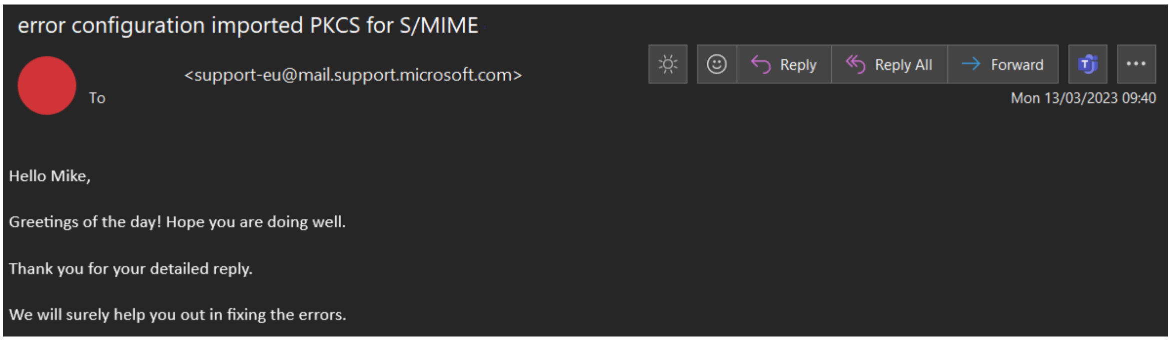
So I'm advised to figure out if the KeyTalk Certificate and Key Management Solution actually did its job properly and got an S/MIME certificate and key in PFX format ready for Intune to install onto a managed device?

It seems Microsoft's online environment isn't much help and requires me to reach out to the Reddit community. Long story short, after a few days I figure it out, and Intune shows me:


```
Id                                                                        CreatedDateTime     EncryptedPfxBlob EncryptedPfxPassword ExpirationDateTime  IntendedPurpose KeyName
--                                                                        ---------------     ---------------- -------------------- ------------------  --------------- -------
aeeeaebf116248699b9d8bc8da9263c2-4b192c373a39d4e30884ae33b60908a94c89aeba 13/03/2023 10:31:39 {0}                                   08/09/2023 14:41:42 unassigned      PFXEncryptionKey
97186ee1c06e4edc83fdb62f2c563135-3d5002db357e037c78030797b24a7bc1eebba796 27/03/2023 16:51:15 {0}                                   22/03/2024 13:10:39 unassigned      PFXEncryptionKey
b8c5f4efa2674068b965e99c0b62e737-ef740034ead3495718e940e58ddd847c3dec119d 17/02/2023 15:08:42 {0}                                   26/03/2023 13:20:53 unassigned      PFXEncryptionKey
b8c5f4efa2674068b965e99c0b62e737-fc4987d1c5b173007fa358a73da110eb12610046 23/02/2023 13:21:57 {0}                                   24/02/2024 13:21:50 unassigned      PFXEncryptionKey

PS C:\Windows\System32>
```

Total abracadabra looking at the Ids, but for Microsoft Support it suffices to prove the issue is in Intune and not in the pre-provisioning.


error configuration imported PKCS for S/MIME

<support-eu@mail.support.microsoft.com>

To

Mon 13/03/2023 09:40

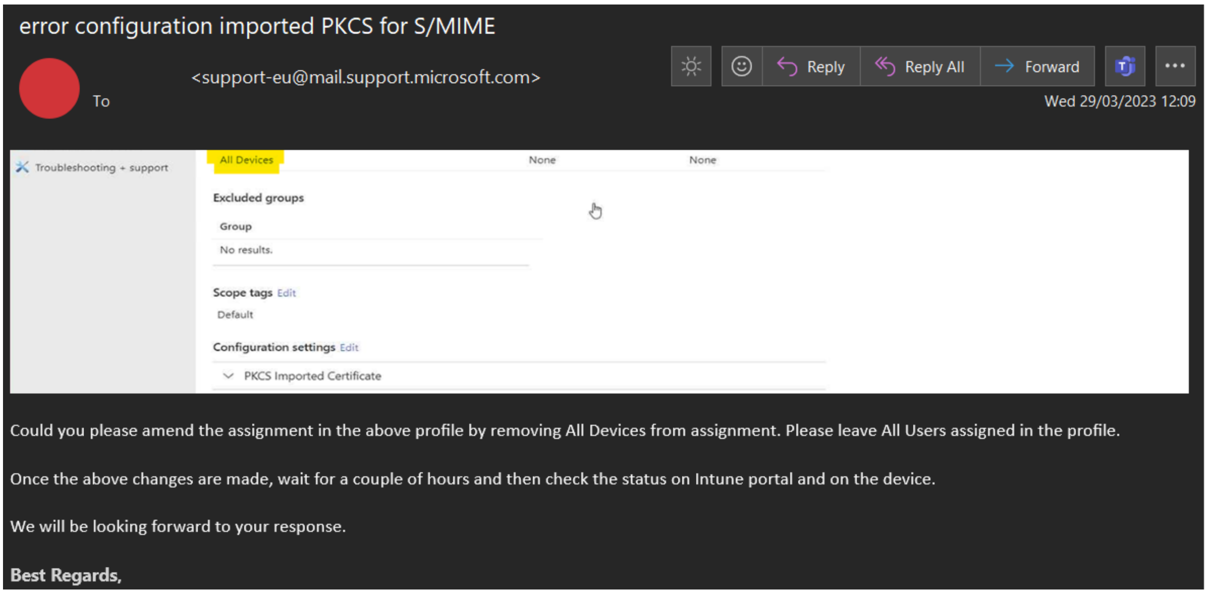
Hello Mike,

Greetings of the day! Hope you are doing well.

Thank you for your detailed reply.

We will surely help you out in fixing the errors.

And after various follow ups:



error configuration imported PKCS for S/MIME

<support-eu@mail.support.microsoft.com>

To

Wed 29/03/2023 12:09

All Devices	None	None

Excluded groups

Group
No results.

Scope tags Edit

Default

Configuration settings Edit

PKCS Imported Certificate

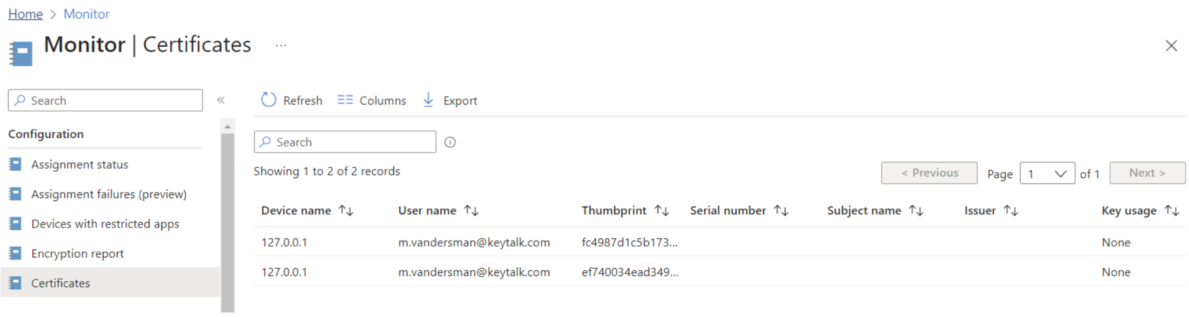
Could you please amend the assignment in the above profile by removing All Devices from assignment. Please leave All Users assigned in the profile.

Once the above changes are made, wait for a couple of hours and then check the status on Intune portal and on the device.

We will be looking forward to your response.

Best Regards,

Success! :



Home > Monitor

Monitor | Certificates

Showing 1 to 2 of 2 records

Device name	User name	Thumbprint	Serial number	Subject name	Issuer	Key usage
127.0.0.1	m.vandersman@keytalk.com	fc4987d1c5b173...				None
127.0.0.1	m.vandersman@keytalk.com	ef740034ead349...				None

Configuring Outlook Mobile: another support ticket… that’s for another story

S/MIME certificates are being properly distributed, but for some reason they do show properly in Outlook Mobile for Android, but not in Outlook Mobile for iOS? How’s that even possible? That’s for another future blog post to explain. 😊

Epilogue: Certificate management with Intune

The above issues were resolved, albeit for our business environment based on our encountered issues.

It's always important to never put all your eggs in one basket, so definitely reach out to Microsoft Support. While they do take their time, they do get the issues most of the time resolved.

But also don't hesitate to reach out to KeyTalk support, as we've dealt with hundreds of issues with customers using Intune, and can often provide relevant help or at least provide hints that will help resolve the issue faster.

If you have any questions about this whitepaper or any other question related to certificate management with Microsoft Intune, please contact us.

KeyTalk IT Security Software B.V.
website: keytalk.com
email: info@keytalk.com

Central office:

Maanlander 47
3824 MN Amersfoort
The Netherlands

Phone: +31 88 539 82 55