

Exploiting the 0365 Duo 2FA Misconfiguration

Cassandra Young

@muteki_rtw

muteki

- ▶ Senior Scientist (R&I - Cloud Security)
@ Security Risk Advisors
- ▶ Grad Student in Computer Science
@ University of Pennsylvania
- ▶ Blue Team Village Organizer
- ▶ Lives for international travel, scuba diving,
woodworking, jigsaw puzzles and baking

Cassandra Young (she/her)

Twitter: @muteki_rtw

LinkedIn: [linkedin.com/in/cassandray](https://www.linkedin.com/in/cassandray)

GitHub: github.com/muteki-apps



Scope

- ▶ Office 365 on Azure Tenant
- ▶ Basic authentication not fully blocked
- ▶ 2 Factor Authentication via Duo
- ▶ Configuration most likely implemented prior to August 2020

Background

- ▶ O365 Authentication Types:
 - ▶ Legacy: Basic auth, protocols that send username and password
 - ▶ Modern: client/server authentication, with access & refresh tokens
- ▶ Email Protocols:
 - ▶ POP, IMAP, SMTP
 - ▶ ActiveSync
 - ▶ MAPI/RPC

MFA/2FA requires modern authentication

[mis]configuration

Part 1) Duo Configuration

- ▶ Duo is not part of the misconfiguration
- ▶ Duo's documentation explicitly notes that the prompt will only trigger on clients that support modern authentication!

2) Conditional Access Policies in Azure Active Directory

- ▶ A Conditional Access policy consists of:
 - ▶ Assignments
 - ▶ Users/groups
 - ▶ Cloud Apps or Actions
 - ▶ Conditions
 - ▶ Access
 - ▶ Grant or Deny
 - ▶ 'Grant' is where Duo integration gets triggered

Diving into Conditions

- ▶ The 'client apps' option under 'conditions' lets you filter by app protocols
- ▶ Exchange ActiveSync is listed separately
- ▶ If not checked, Duo policy will not apply
- ▶ Another approach: 2nd CA policy blocks basic auth (and often leaves out ActiveSync)

...but this isn't as straightforward as it looks

The screenshot shows the 'MFA my login' Conditional Access policy configuration page. The policy is currently 'Not configured'. The 'Name' field is 'MFA my login'. Under 'Assignments', 'Users and groups' is set to 'Specific users included', 'Cloud apps or actions' is set to '1 app included', and 'Conditions' is set to '1 condition selected'. Under 'Access controls', 'Grant' is set to '1 control selected' and 'Session' is set to '0 controls selected'. The 'Client apps' section on the right is expanded, showing a 'Configure' toggle set to 'Yes'. Below the toggle, it says 'Select the client apps this policy will apply to'. Under 'Modern authentication clients', 'Browser' and 'Mobile apps and desktop clients' are checked. Under 'Legacy authentication clients', 'Exchange ActiveSync clients' is unchecked and 'Other clients' is checked.

MFA my login ...
Conditional Access policy

Delete

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
MFA my login

Assignments

Users and groups ⓘ
Specific users included

Cloud apps or actions ⓘ
1 app included

Conditions ⓘ
1 condition selected

Access controls

Grant ⓘ
1 control selected

Session ⓘ
0 controls selected

Control user access based on signals from conditions like risk, device platform, location client apps, or device state. [Learn more](#)

User risk ⓘ
Not configured

Sign-in risk ⓘ
Not configured

Device platforms ⓘ
Not configured

Locations ⓘ
Not configured

Client apps ⓘ
3 included

Filters for devices (Preview) ⓘ
Not configured

Client apps ✕

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ
Yes No

Select the client apps this policy will apply to

Modern authentication clients

☒ Browser

☒ Mobile apps and desktop clients

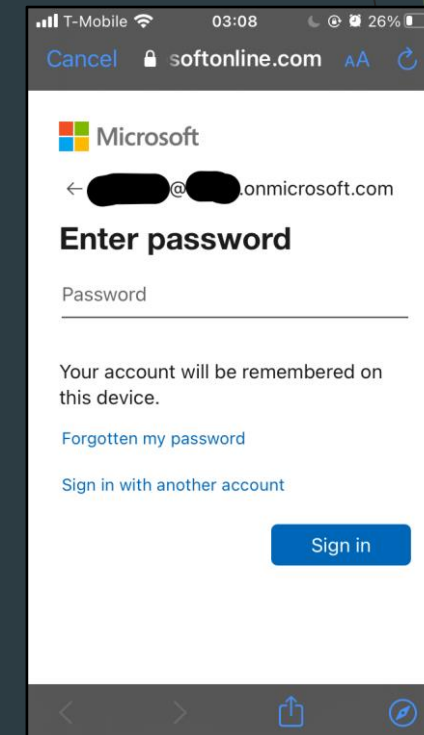
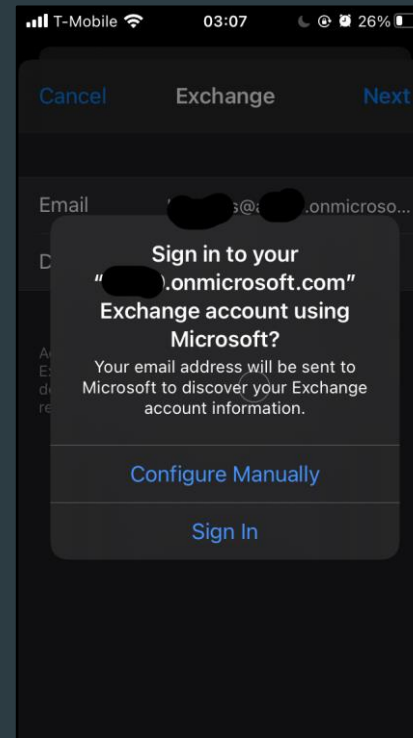
Legacy authentication clients

☐ Exchange ActiveSync clients ⓘ

☒ Other clients ⓘ

Use Case: Apple's iOS Mail App

- ▶ Normal sign-in via iOS settings:
 - ▶ Add “Microsoft Exchange” account
 - ▶ Hit next and “sign in”
 - ▶ Microsoft-branded prompt pops up and asks for the password
 - ▶ After signing in, Duo prompt shows up

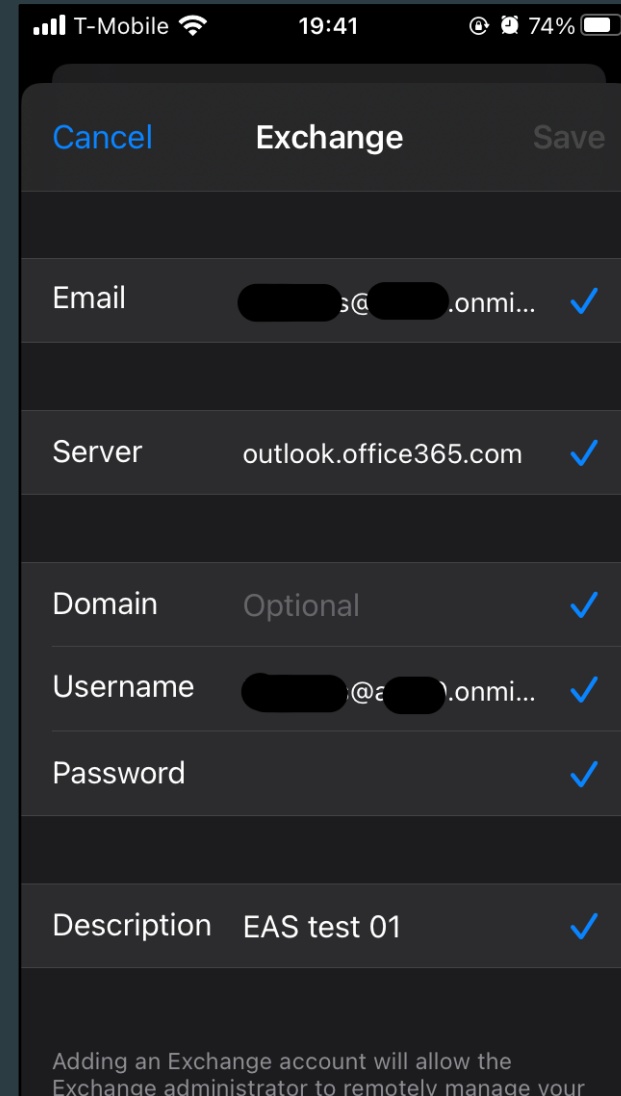


iOS will default to a modern authentication prompt

Apple's iOS Mail App - Forcing ActiveSync

- ▶ Add “Microsoft Exchange” account
- ▶ Hit next and either:
 - ▶ 1) “sign in” but cancel prompt, enter password
 - ▶ 2) configure manually

That's it.



Programmatic Access

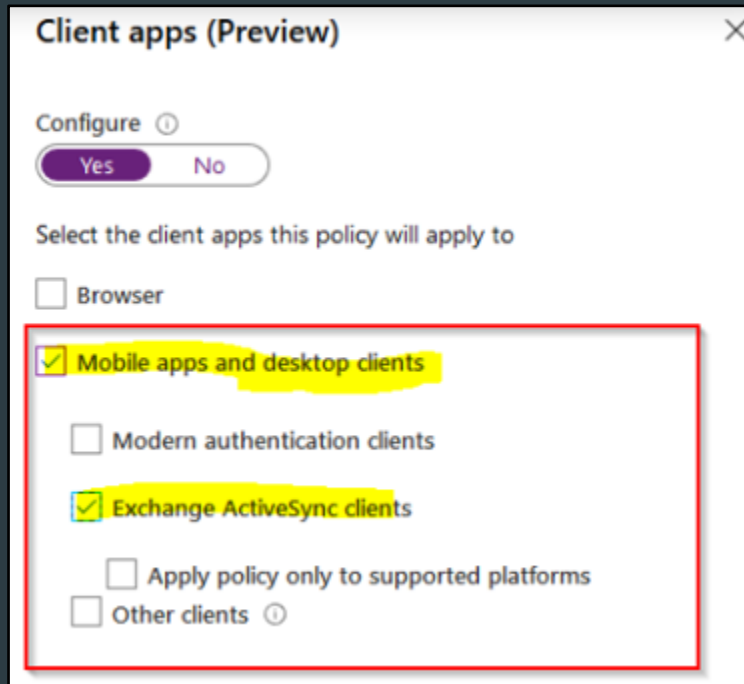
- ▶ Apps using ActiveSync are easy to find on GitHub/GitLab
- ▶ ActiveSync is a simple authentication protocol:
HTTP request header contains base64-encoded {"Authorization" : "Basic " +
username:password}
- ▶ ActiveSync gives client access to email, contacts, calendars, & more

The background features a dark blue-grey field on the left, transitioning into a series of overlapping, semi-transparent green and yellow-green geometric shapes on the right. These shapes are primarily triangles and polygons, creating a layered, abstract effect. The word "explanation" is centered in the dark blue area.

explanation

1) Previous wording of ActiveSync

Option prior to August 2020



Client apps (Preview) [Close]

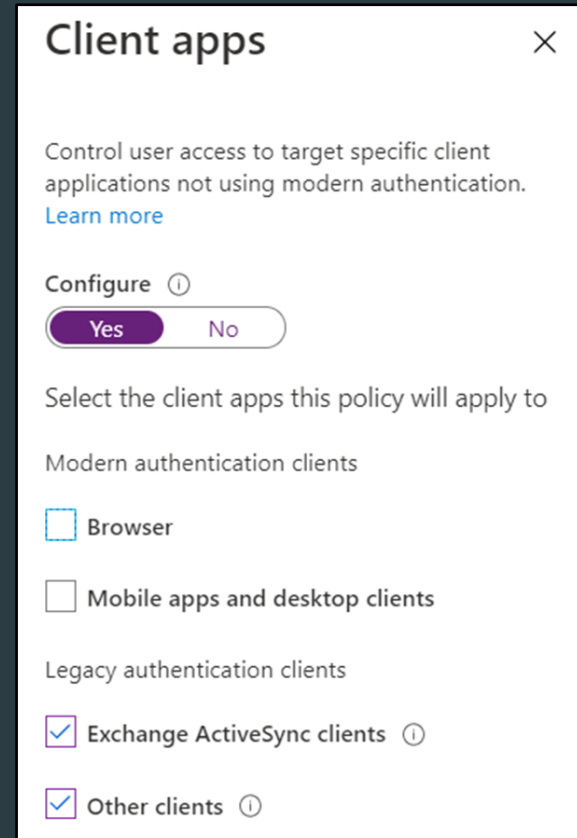
Configure ⓘ

Yes No

Select the client apps this policy will apply to

- ☐ Browser
- ☒ Mobile apps and desktop clients
- ☐ Modern authentication clients
- ☒ Exchange ActiveSync clients
- ☐ Apply policy only to supported platforms
- ☐ Other clients ⓘ

Updated version



Client apps [Close]

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ

Yes No

Select the client apps this policy will apply to

Modern authentication clients

- ☐ Browser
- ☐ Mobile apps and desktop clients

Legacy authentication clients

- ☒ Exchange ActiveSync clients ⓘ
- ☒ Other clients ⓘ

2) Client Apps left Preview

- ▶ New Conditional Access policies will now apply to all client app types
 - ▶ Before August 2020: “Conditional Access policies by default apply to browser-based applications and applications that utilize modern authentication protocols.”
- ▶ Importantly:
 - ▶ “The behavior of the client apps condition was updated in August 2020. If you have existing Conditional Access policies, they will remain unchanged.”



detect & remediate

Detection in Azure Active Directory

- ▶ Search Sign-Ins for Client App - “Exchange ActiveSync”
- ▶ ActiveSync fully re-authenticates on access, so you’ll see frequent logs

Activity Details: Sign-ins

Basic info Location Device info Authentication Details **Conditional Access** Report-only Additional Details

Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓
MFA my login	RequireDuoMfa		Not Applied ...

A sign-in can also be interrupted (e.g. blocked, MFA challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

Activity Details: Sign-ins

Basic info Location Device info Authentication Details Conditional Access Report-only Additional Details

Date	8/5/2021, 1:37:17 AM	User	
Request ID	038141a9-95f6-411f-b4a6-0cf7dc75f101	Username	
Correlation ID	b85814bb-52ff-4296-8778-5644716bbaba	User ID	
Authentication requirement	Single-factor authentication	Sign-in identifier	
Status	Success	User type	
Continuous access evaluation	No	Cross tenant access type	

Application	Office 365 Exchange Online
Application ID	00000002-0000-Off1-ce00-000000000000
Resource	Office 365 Exchange Online
Resource ID	
Resource tenant ID	
Home tenant ID	
Client app	Exchange ActiveSync

Token issuer type	Azure AD
Token issuer name	
Latency	153ms
Flagged for review	No
User agent	Apple-iPhone8C4/1806.72

Example: Detection in Splunk

- ▶ `index=<your index> ClientInfoString="Client=Microsoft.Exchange.ActiveSync*" | dedup ClientInfoString,UserId | table UserId, ClientInfoString, ClientIP, _time`
- ▶ Sign-in logs are more accurate here than in the Azure Portal

Client app	Conditional Access
Exchange ActiveSync	Success
Exchange ActiveSync	Success
Exchange ActiveSync	Success

Activity Details: Sign-ins

Basic info

Location

Device info

Authentication Details

Conditional Access

Report-only

Additional Details

Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓	
	RequireDuoMfa		Not Applied	...

...pted (e.g. blocked, MFA challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only cies.

Remediation 1:

Tweak Conditional Access Policy

- ▶ Check the ActiveSync box in your Duo policy
 - ▶ a Conditional Access *Grant* will *block* legacy authentication
 - ▶ If implementing a CA policy to explicitly block basic auth, the same applies!
- ▶ Or, remove Client Apps Configure option entirely
- ▶ End behavior: Client can authenticate via ActiveSync over basic auth, but can't view: no authorization

Note: you can create new policy to test before deploying, and enable it in report-only mode

Client apps

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ

☐ Yes ☒ No

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser

☐ Mobile apps and desktop clients

Legacy authentication clients

☐ Exchange ActiveSync clients ⓘ

☐ Other clients ⓘ

i When not configured, policies now apply to all client apps, including modern and legacy auth.

Remediation 2: Disable Legacy Auth

Legacy Auth is (Almost) Dead

- ▶ Microsoft's plans to disable legacy authentication were delayed by the pandemic.
- ▶ Basic auth disabled for:
 - ▶ New tenants
 - ▶ Existing tenants with zero use of basic auth
- ▶ Microsoft provides instruction on blocking legacy auth, including ActiveSync:
 - ▶ <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

... but you'd be surprised how many O365 tenants are still widely using it!

Thanks!

- ▶ Find me on Twitter! @muteki_rtw
- ▶ Slides will be posted on GitHub: github.com/muteki-apps