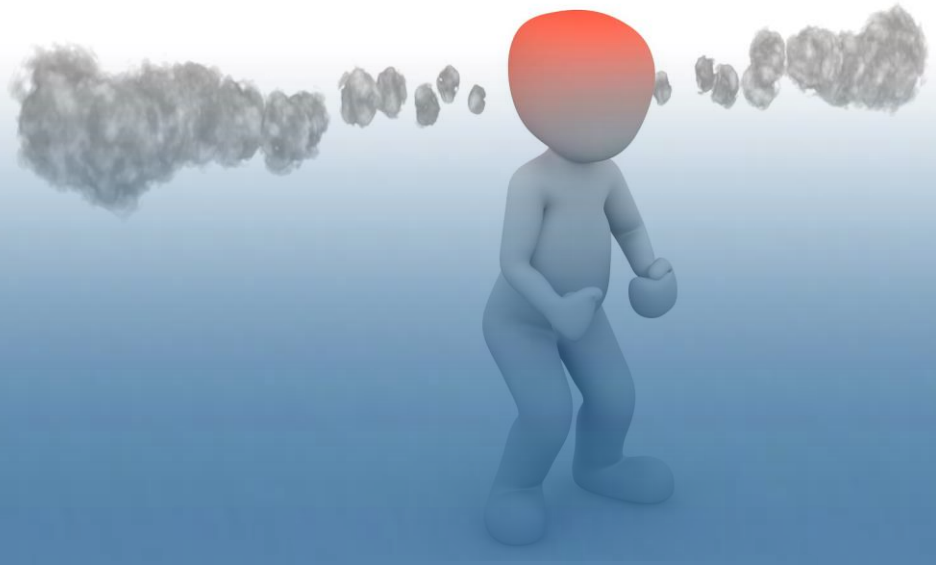
February 6th-7th

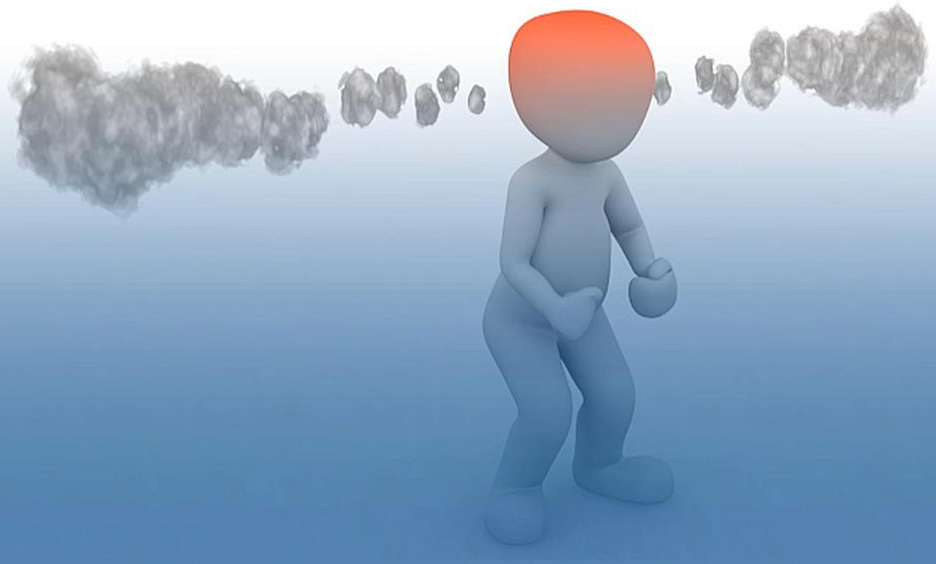
NIC 20/20 VISION

Oslo Spektrum

Securing identity without annoying users



Securing identity without annoying users



Free

Get your New Iphone 12 #4Free

As Good as free

Congratulation you're a Winner (Even without participating)

Offer Valid for 1 Hour, Only For You

make it SUCCESS MONEY WORK LIFE VIDEO

SPEND

‘Nigerian prince’ email scams still over $700,000 a year—here’s how protect yourself

Published Thu, Apr 18 2019·2:38 PM EDT

Megan Leonhardt
@MEGAN_LEONHARDT

Share

Twenty20

The “Nigerian prince” email scam is perhaps one of the longest-running Internet frauds. Actress Anne Hathaway even joked about it in her monologue on “Saturday Night Live” over a decade ago.

Also called “Nigerian letter” scams or “foreign money exchanges,” these

https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams

ACCC AUSTRALIAN COMPETITION & CONSUMER COMMISSION SCAMWATCH

Enter a search term

Types of scams | Report a scam | Get help | News | About Scamwatch

Home > Types of scams > Unexpected money

Listen

Nigerian scams

Nigerian scams involve someone overseas offering you a share in a large sum of money or a payment on the condition you help them to transfer money out of their country. While these scams originated in Nigeria, they now come from all over the world.

How this scam works

The scammer will contact you out of the blue by email, letter, text message or through social media.

The scammer will tell you an elaborate story about large amounts of their money trapped in banks during events such as civil wars or coups, often in countries currently in the news. Or they may tell you about a large inheritance that is 'difficult to access' because of government restrictions or taxes in their country. The scammer will then offer you a large sum of money to help them transfer their personal fortune out of the country.

These scams are often known as 'Nigerian 419' scams because the first wave of them came from Nigeria. The '419' part of the name comes from the section of Nigeria's Criminal Code which outlaws the practice. These scams now come from anywhere in the world.

Scammers may ask for your bank account details to 'help them transfer the money' and use this information to later steal your funds.

Report this scam

Nigerian scams statistics

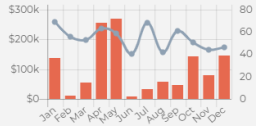
- 2019 -

Amount lost
$1 245 631

Number of reports
652

Reports with financial losses
22.1%

Amount lost & reports



Number of reports Amount lost

Identity

- Identity Theft
  - Personal threat
  - Organizational threat
- Identity
  - Foundation for:
    - Personal digital life
    - Professional digital life

The User Complexity Challenge - Generations

- The Lost Generation
- The G.I. Generation
- The Silent Generation
- The Baby Boomers
- Generation X
- Generation Y (Millennials)
- Generation Z

The Baby Boomers

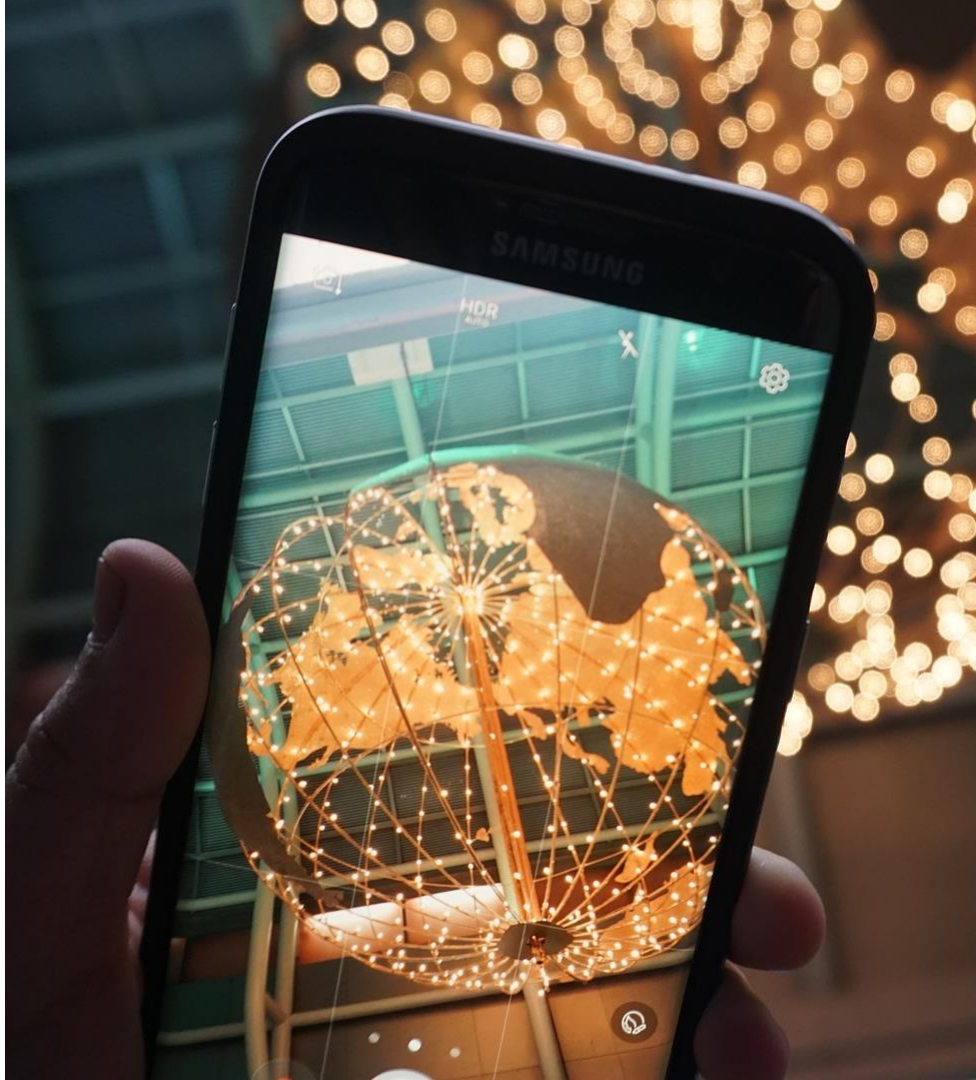
- The “helpful”
- Skilled
- Unafraid of doing mistakes
- Average
- Afraid of doing mistakes
- Technology Challenged

Generation X

- The “helpful”
- Skilled
- Average
- Technology Challenged

Millennials

- Too Skilled
- Skilled (Average)
- Technology Challenged



Post-Millennials

- First real “futuristic user” Only modern / hight tech user group
- Grownup with smartphones and taplets (iphone 2007/Ipad 2010). Late Windows XP and more affected by Win 7
- Technology Wise few(er) sub categories. Everybody have quite extended experience as technology consumer

Other factors with the user complexity challenge

- Background
- Interesse
- Influence
- Education
- Etc.

Standard Users
E3 Level

But first, Free stuff

Azure MFA Free

Feature	Azure AD Free - Security defaults	Azure AD Free - Azure AD Global Administrators	Office Premium, E3, or E5	Azure AD Premium P1 or P2
Protect Azure AD admin accounts with MFA	●	● (Azure AD Global Administrator accounts only)	●	●
Mobile app as a second factor	●	●	●	●
Phone call as a second factor		●	●	●
SMS as a second factor		●	●	●
Admin control over verification methods		●	●	●
Fraud alert				●
MFA Reports				●
Custom greetings for phone calls				●
Custom caller ID for phone calls				●
Trusted IPs				●
Remember MFA for trusted devices		●	●	●
MFA for on-premises applications				●

Keywords

Training

Inspiration

Motivation

Respect

At the Office

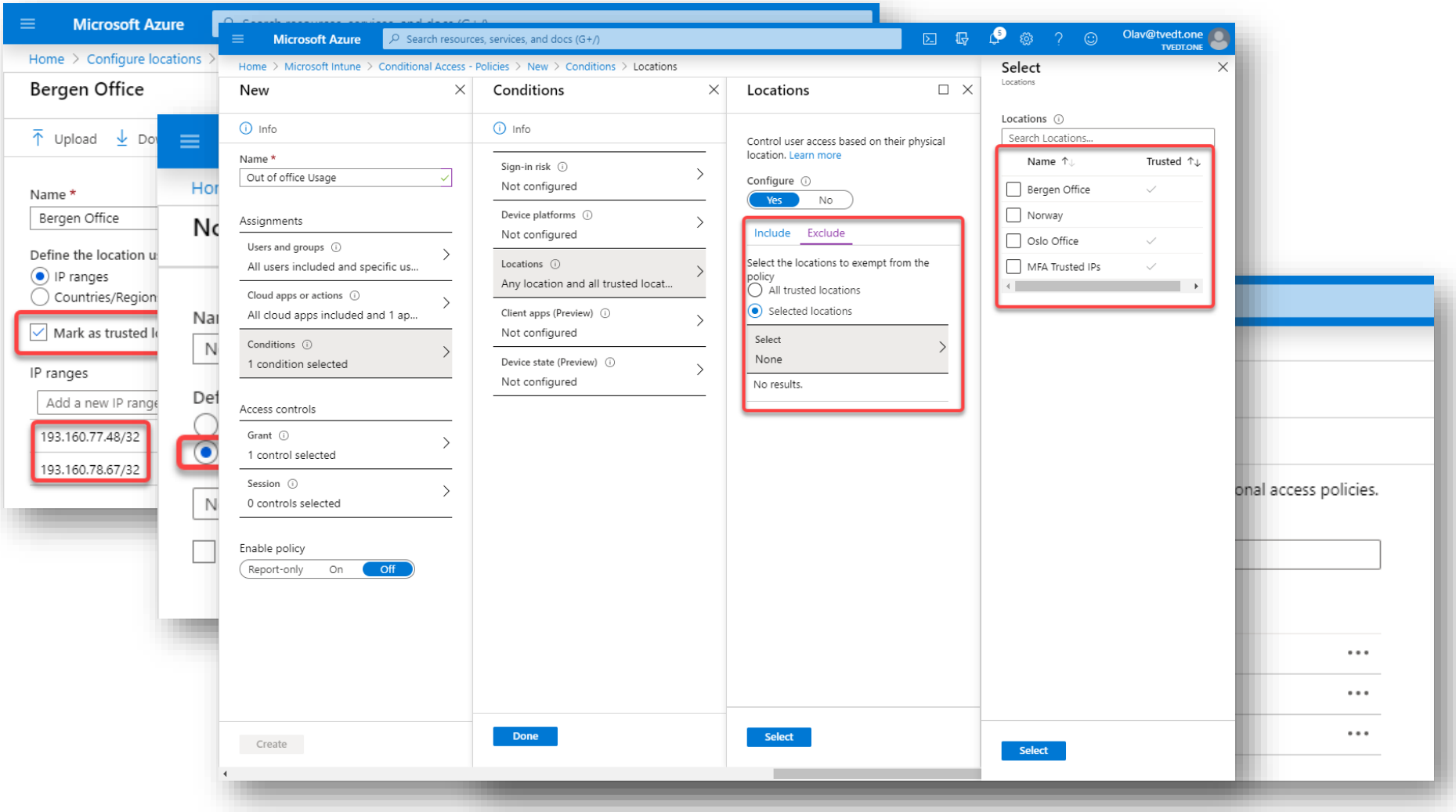
Business as usual

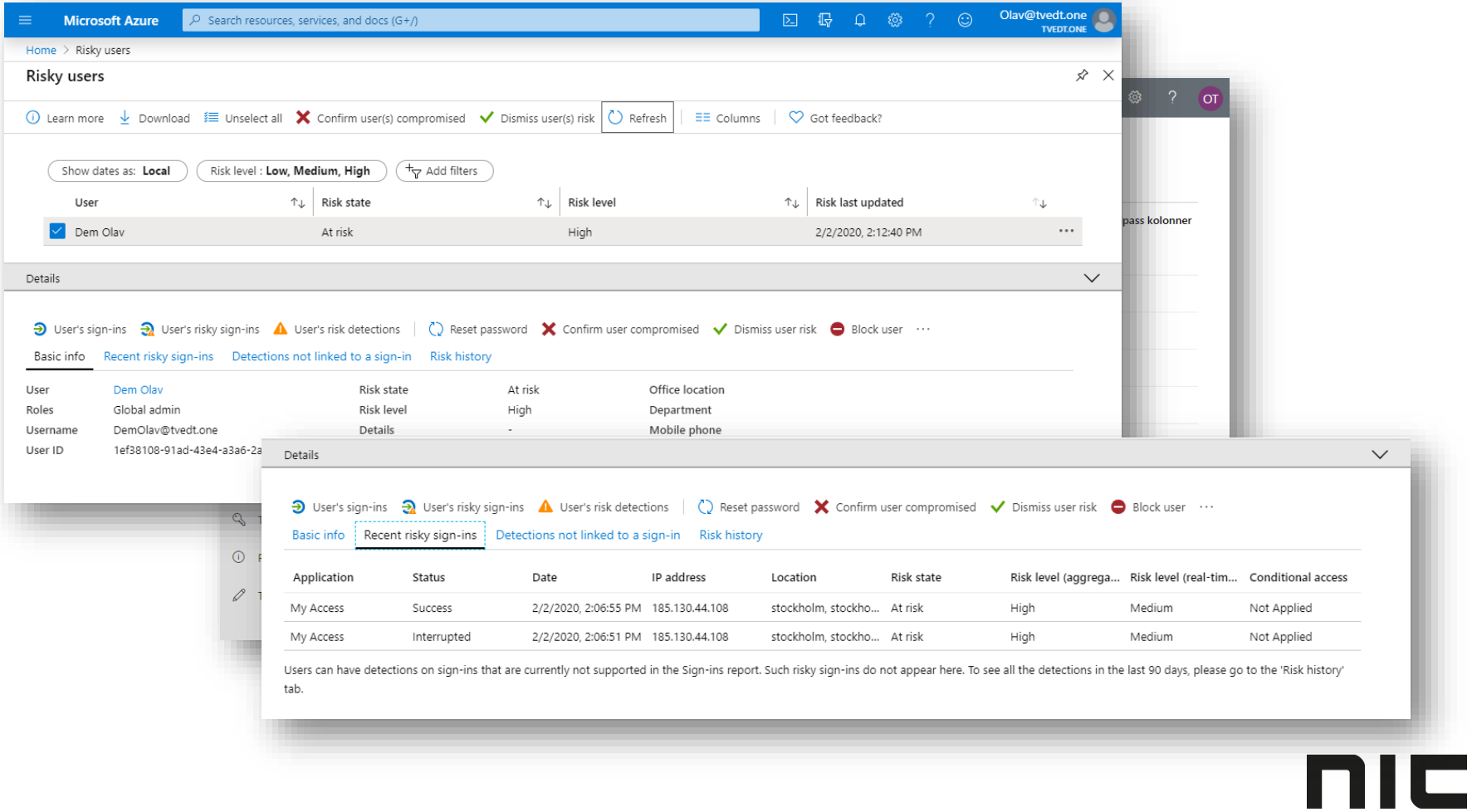
- No extra visual security measure
- No hassle

Not at the Office / In the country

Extra security measures

- Conditional Access
  - MFA
  - Device State
  - App protection policy
  - Approved client apps


Microsoft Azure
Home > Configure locations
Bergen Office
Upload
Name *
Bergen Office
Define the location u
IP ranges
Countries/Region
Mark as trusted l
IP ranges
Add a new IP range
193.160.77.48/32
193.160.78.67/32
Microsoft Azure
Search resources, services, and docs (G+/)
Olav@tvedt.one
TVEDT.ONE
Home > Microsoft Intune > Conditional Access - Policies > New > Conditions > Locations
New
Info
Name *
Out of office Usage
Assignments
Users and groups
All users included and specific us...
Cloud apps or actions
All cloud apps included and 1 ap...
Conditions
1 condition selected
Access controls
Grant
1 control selected
Session
0 controls selected
Enable policy
Report-only
On
Off
Create
Conditions
Info
Sign-in risk
Not configured
Device platforms
Not configured
Locations
Any location and all trusted locat...
Client apps (Preview)
Not configured
Device state (Preview)
Not configured
Done
Locations
Control user access based on their physical location. Learn more
Configure
Yes
No
Include
Exclude
Select the locations to exempt from the policy
All trusted locations
Selected locations
Select
None
No results.
Select
Select
Locations
Locations
Search Locations...
Name
Trusted
Bergen Office
Norway
Oslo Office
MFA Trusted IPs
Select
onal access policies.


Microsoft Azure
Search resources, services, and docs (G+/)
Olav@tvedt.one
TVEDT.ONE
Home > Risky users
Risky users
Learn more
Download
Unselect all
Confirm user(s) compromised
Dismiss user(s) risk
Refresh
Columns
Got feedback?
Show dates as: Local
Risk level : Low, Medium, High
Add filters
User
Risk state
Risk level
Risk last updated
Dem Olav
At risk
High
2/2/2020, 2:12:40 PM
Details
User's sign-ins
User's risky sign-ins
User's risk detections
Reset password
Confirm user compromised
Dismiss user risk
Block user
Basic info
Recent risky sign-ins
Detections not linked to a sign-in
Risk history
User
Dem Olav
Roles
Global admin
Username
DemOlav@tvedt.one
User ID
1ef38108-91ad-43e4-a3a6-2a
Risk state
At risk
Risk level
High
Details
-
Office location
Department
Mobile phone
Application
Status
Date
IP address
Location
Risk state
Risk level (aggrega...
Risk level (real-tim...
Conditional access
My Access
Success
2/2/2020, 2:06:55 PM
185.130.44.108
stockholm, stockho...
At risk
High
Medium
Not Applied
My Access
Interrupted
2/2/2020, 2:06:51 PM
185.130.44.108
stockholm, stockho...
At risk
High
Medium
Not Applied
Users can have detections on sign-ins that are currently not supported in the Sign-ins report. Such risky sign-ins do not appear here. To see all the detections in the last 90 days, please go to the 'Risk history' tab.

Passwordless Windows Hello And Azure MFA

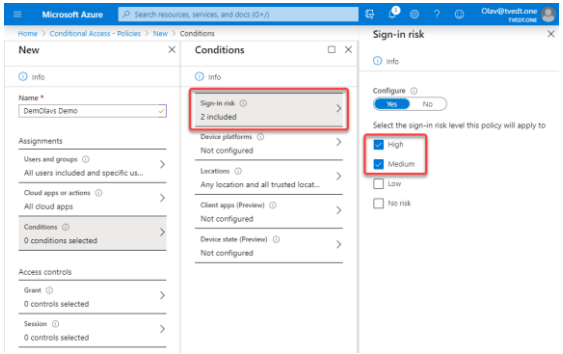
Standard Users
E5 Level

Not at the Office / In the country

Business as usual

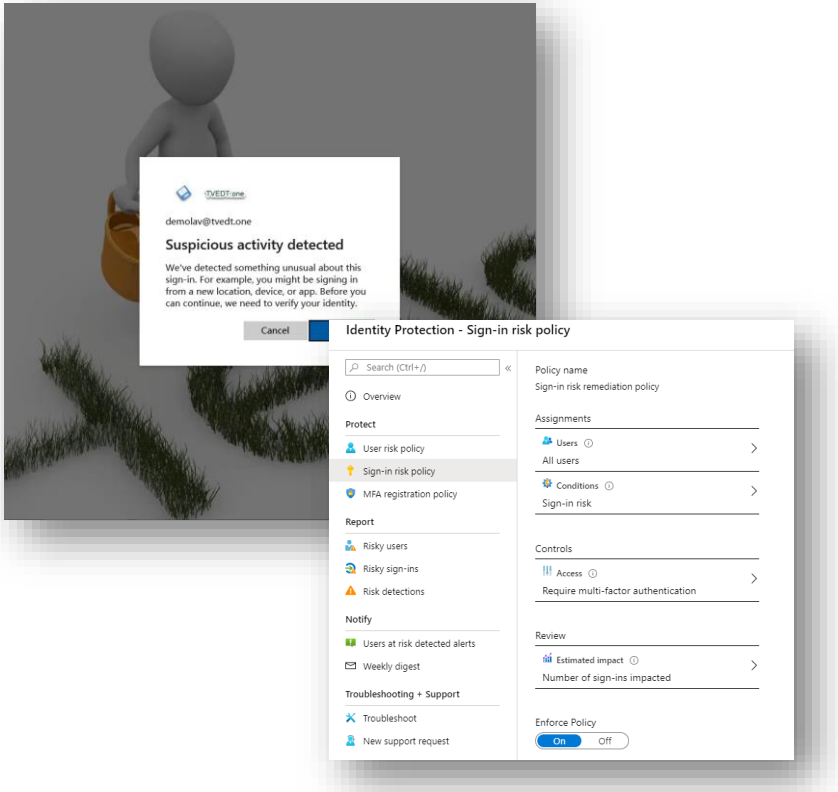
- No extra visual security measure
- No hassle

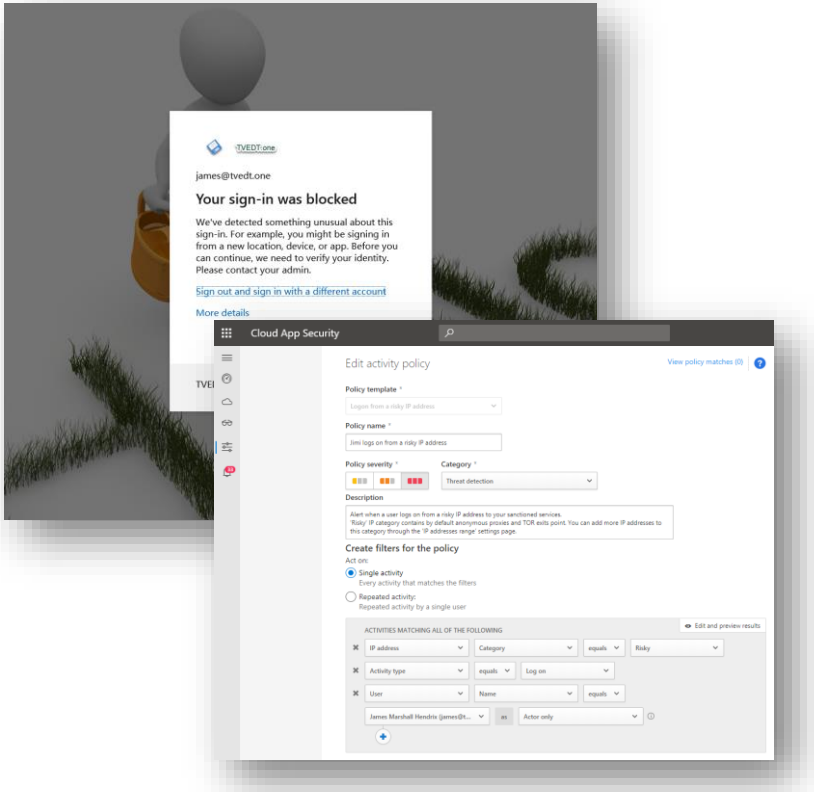
Except if!!!



DEMO

Identity Protection:
Risk Based
MCAS


demolav@tvedt.one
Suspicious activity detected
We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity.
Cancel
Identity Protection - Sign-in risk policy
Search (Ctrl+/)
Overview
Protect
User risk policy
Sign-in risk policy
MFA registration policy
Report
Risky users
Risky sign-ins
Risk detections
Notify
Users at risk detected alerts
Weekly digest
Troubleshooting + Support
Troubleshoot
New support request
Policy name
Sign-in risk remediation policy
Assignments
Users
All users
Conditions
Sign-in risk
Controls
Access
Require multi-factor authentication
Review
Estimated impact
Number of sign-ins impacted
Enforce Policy
On
Off


james@tvedt.one
Your sign-in was blocked
We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin.
Sign out and sign in with a different account
More details
Cloud App Security
Edit activity policy
View policy matches (0)
Policy template
Policy name
Jimi logs on from a risky IP address
Policy severity
Category
Threat detection
Description
Create filters for the policy
Act on:
Single activity
Every activity that matches the filters
Repeated activity:
Repeated activity by a single user
Edit and preview results
ACTIVITIES MATCHING ALL OF THE FOLLOWING
IP address
Category
equals
Risky
Activity type
Log on
User
Name
Actor only

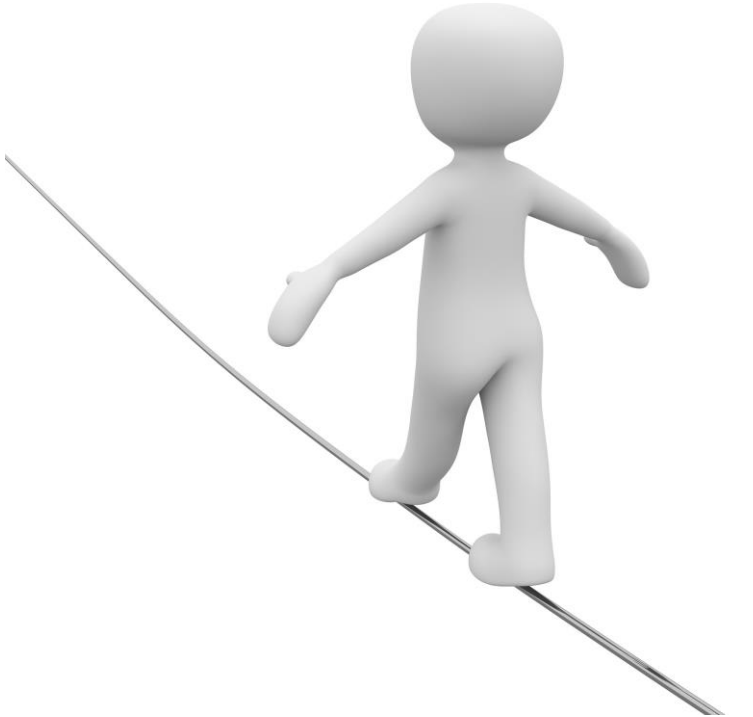
Privileged Users

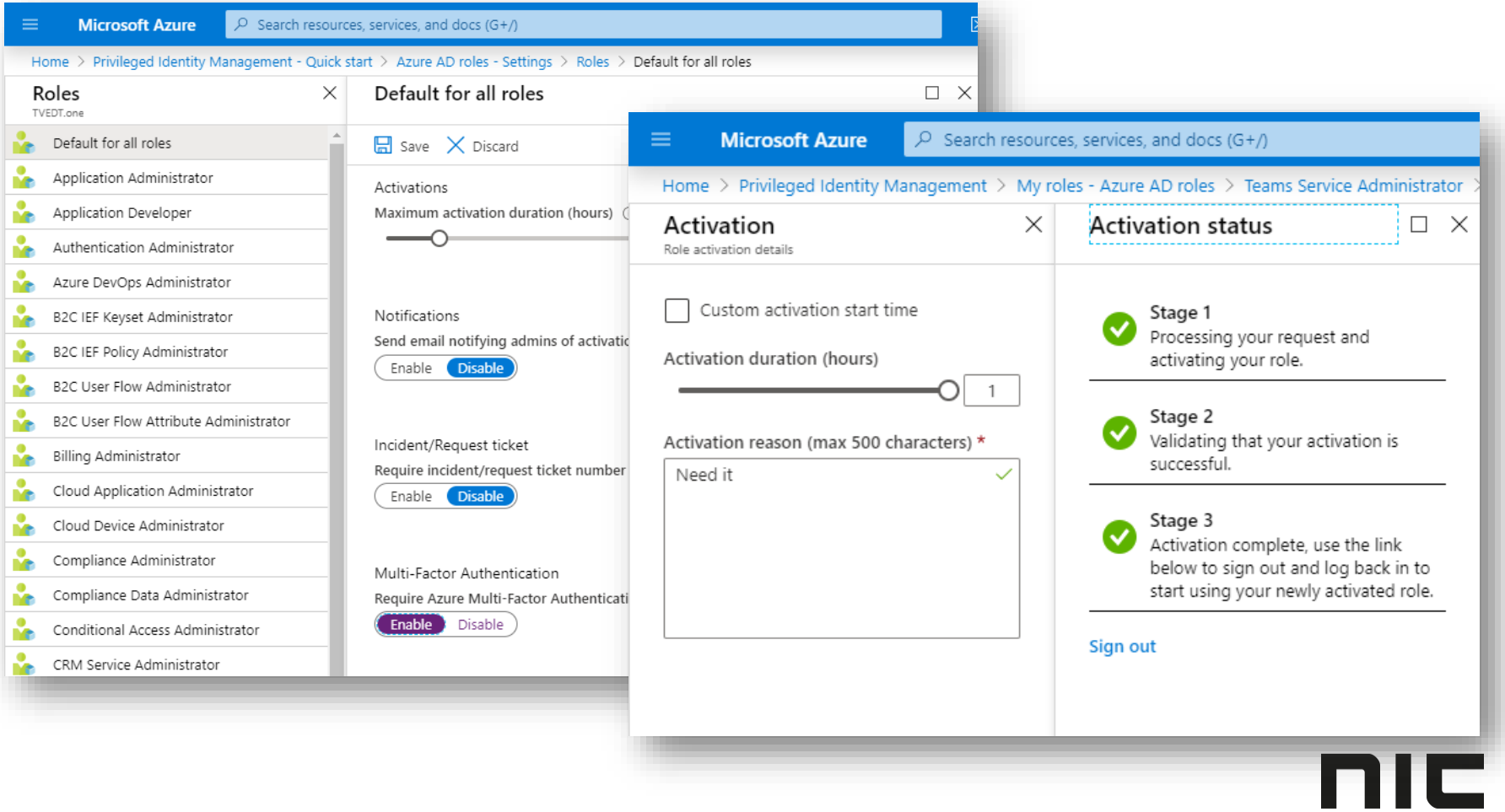
Privileged User

Standard user experience mode

Privileged user mode

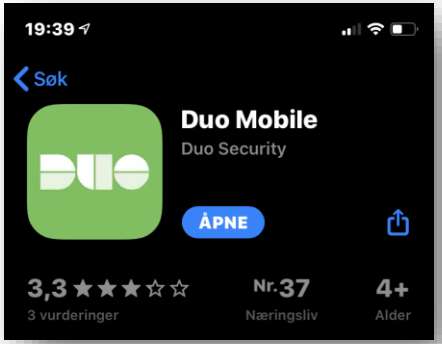
- Conditional Access
  - MFA
- PIM - Privileged Identity Management

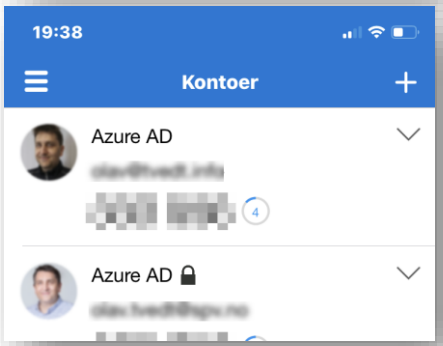


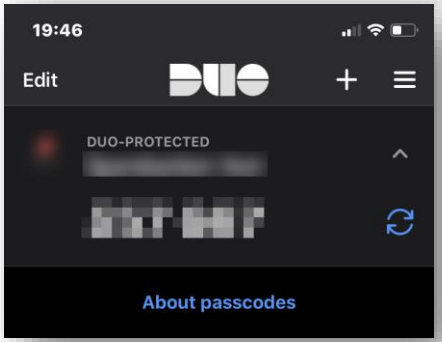

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Privileged Identity Management - Quick start > Azure AD roles - Settings > Roles > Default for all roles
Roles
TVEDT.one
Default for all roles
Application Administrator
Application Developer
Authentication Administrator
Azure DevOps Administrator
B2C IEF Keyset Administrator
B2C IEF Policy Administrator
B2C User Flow Administrator
B2C User Flow Attribute Administrator
Billing Administrator
Cloud Application Administrator
Cloud Device Administrator
Compliance Administrator
Compliance Data Administrator
Conditional Access Administrator
CRM Service Administrator
Default for all roles
Save
Discard
Activations
Maximum activation duration (hours)
Notifications
Send email notifying admins of activatic
Enable
Disable
Incident/Request ticket
Require incident/request ticket number
Enable
Disable
Multi-Factor Authentication
Require Azure Multi-Factor Authenticati
Enable
Disable
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Privileged Identity Management > My roles - Azure AD roles > Teams Service Administrator
Activation
Role activation details
Custom activation start time
Activation duration (hours)
1
Activation reason (max 500 characters) *
Need it
Activation status
Stage 1
Processing your request and activating your role.
Stage 2
Validating that your activation is successful.
Stage 3
Activation complete, use the link below to sign out and log back in to start using your newly activated role.
Sign out

Global Admins and Ninjas

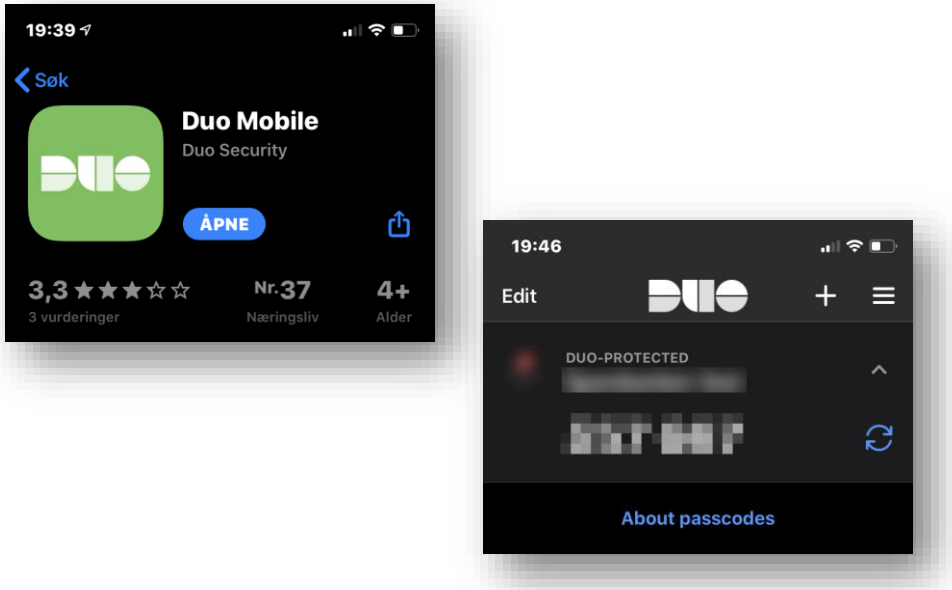
Azure MFA vs DUO

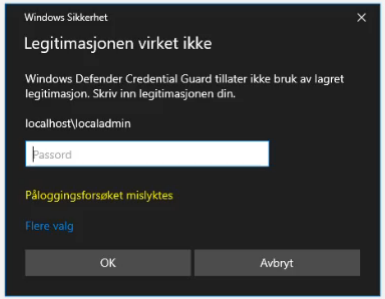






Azure MFA vs DUO

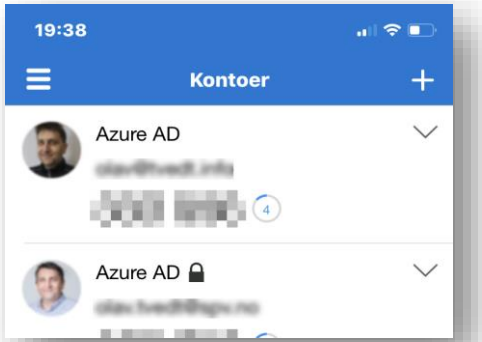



Windows Sikkerhet
Legitimasjonen virket ikke
Windows Defender Credential Guard tillater ikke bruk av lagret legitimasjon. Skriv inn legitimasjonen din.
localhost\localadmin
Passord
Påloggingsforsøket mislyktes
Flere valg
OK
Avbryt

Passwordless

- Windows Hello For Business
- Azure Authenticator App
- Fido2

Passwordless



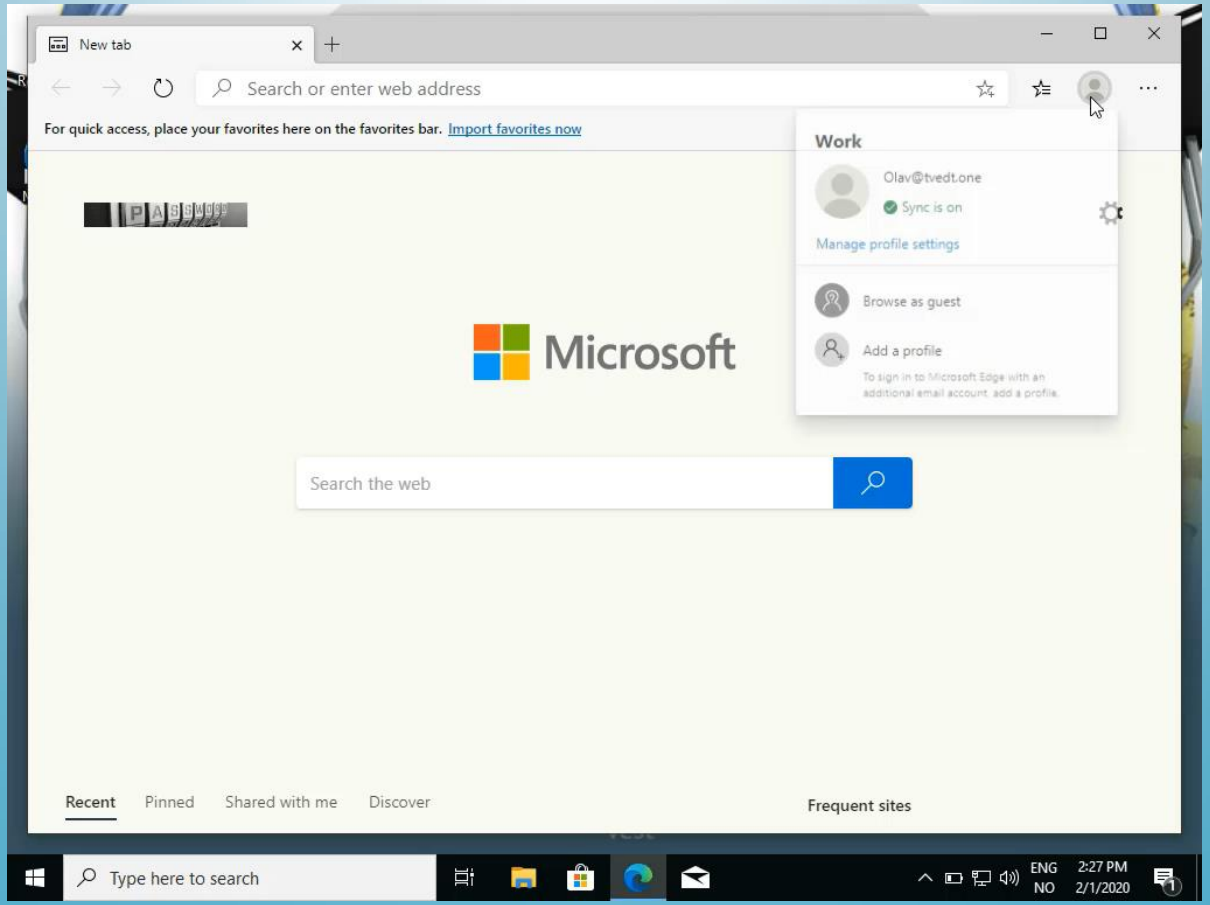
Passwordless

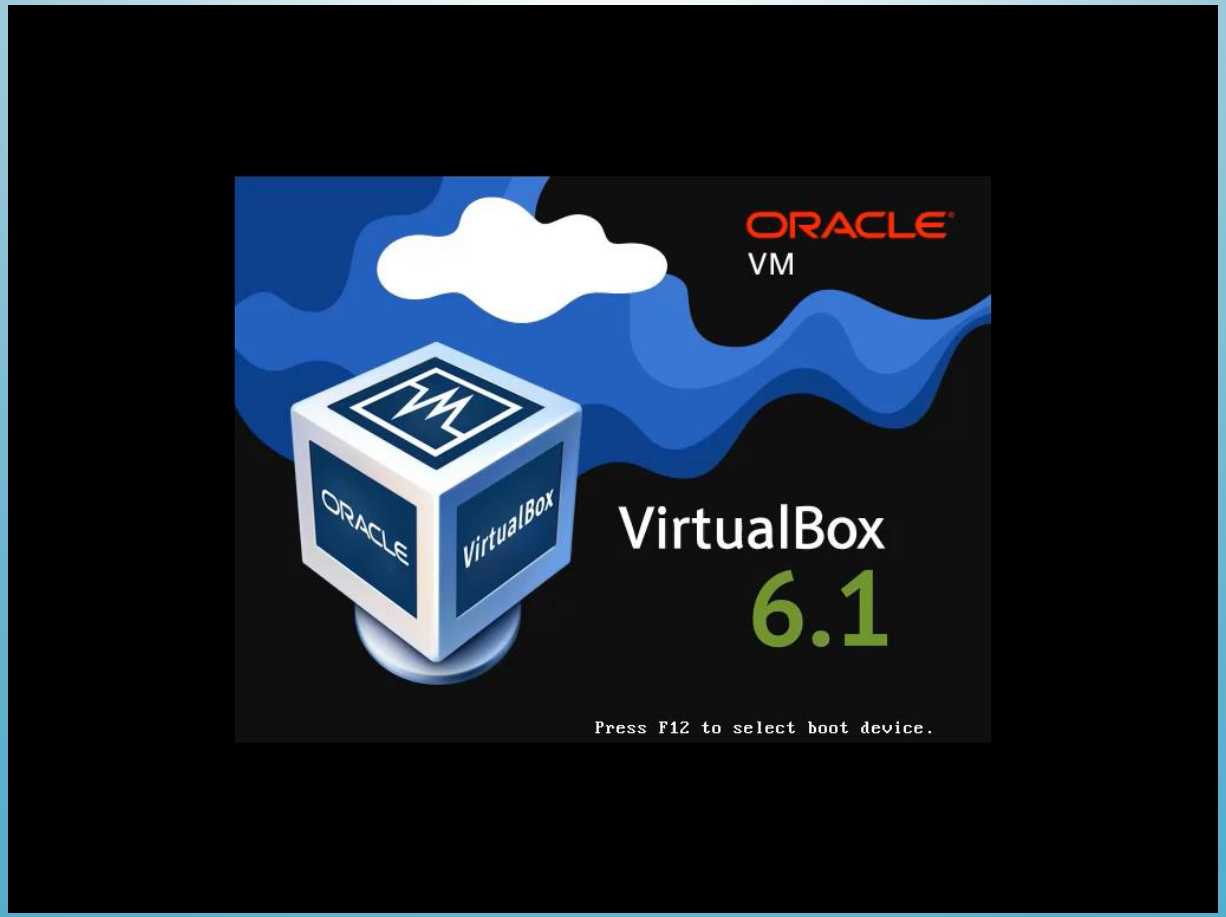
FEITIAN
WE BUILD SECURITY

DEMO

Passwordless

By


New tab
Search or enter web address
For quick access, place your favorites here on the favorites bar. Import favorites now
Work
Olav@tvedt.one
Sync is on
Manage profile settings
Browse as guest
Add a profile
To sign in to Microsoft Edge with an additional email account, add a profile.
Microsoft
Search the web
Recent
Pinned
Shared with me
Discover
Frequent sites
Type here to search
ENG
NO
2:27 PM
2/1/2020


ORACLE
VM
ORACLE
VirtualBox
VirtualBox
6.1
Press F12 to select boot device.

Sum Up

- Adjust after:
  - Role
  - Needs
  - Level
- Automation eases the burden for users while still staying secure

But 2 the most important thing!!!

- Always re-evaluate
- Never say never (Again)

NIC 20/20 VISION

Securing identity without annoying users

Olav Tvedt
Twitter: @olavtwitt
Blog: https://olavtvedt.blogspot.com

Sparebanken Vest

Podcasts: BlåSkjerm Brødrene
PodBean: http://bit.ly/BlaSkj - Apple: http://bit.ly/blaskjerm - Spotify: http://bit.ly/blaaskjerm

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2020