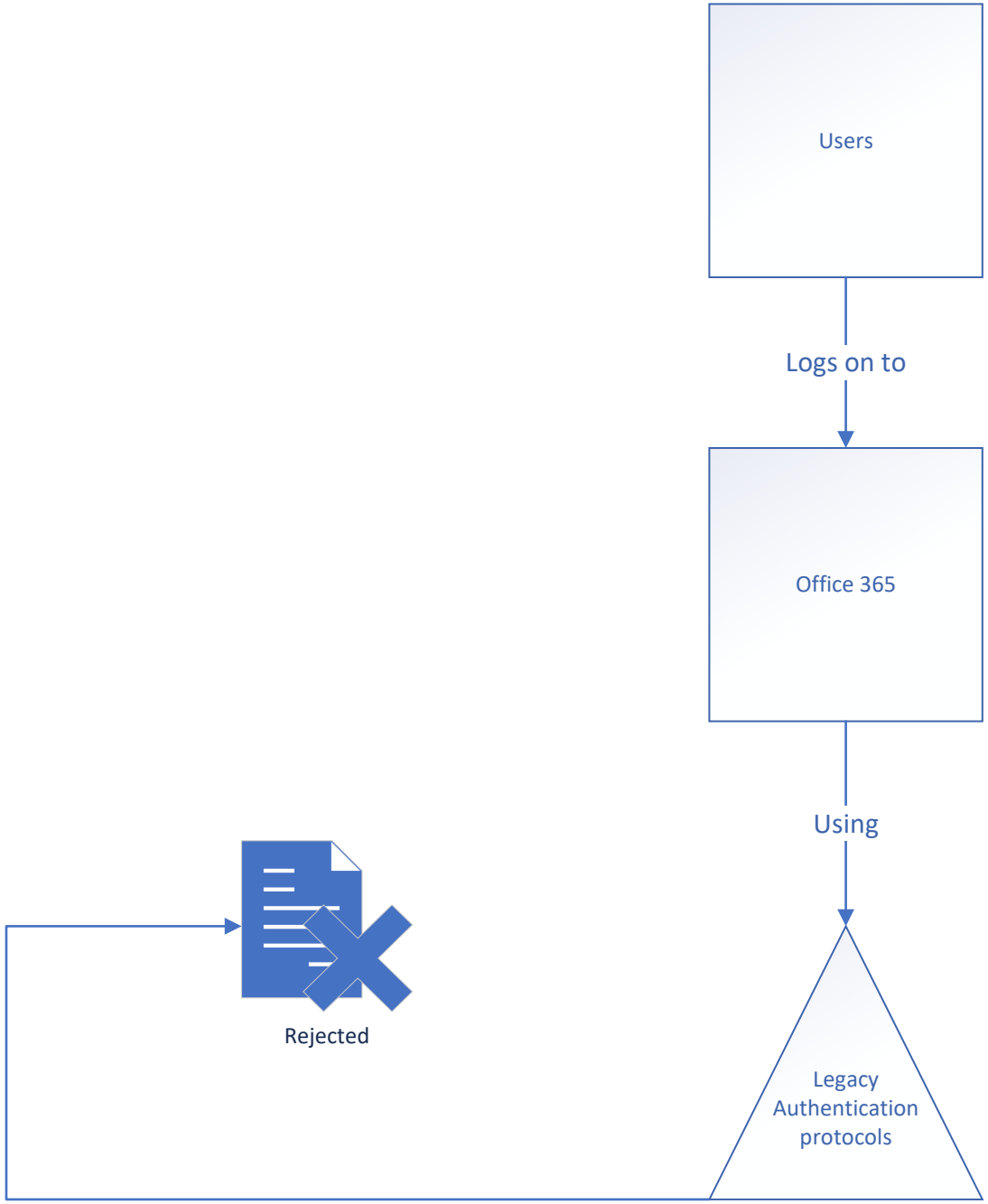
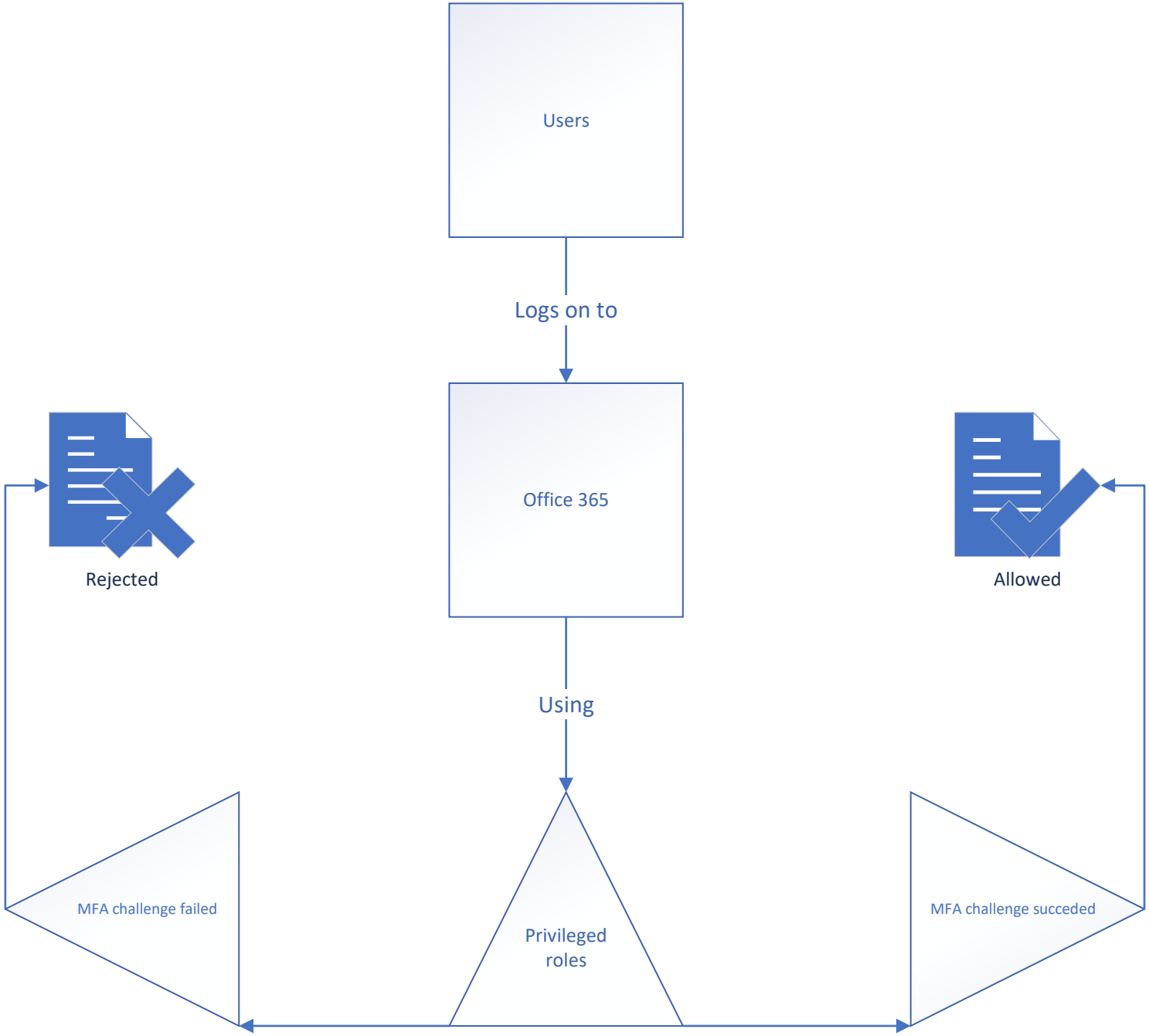
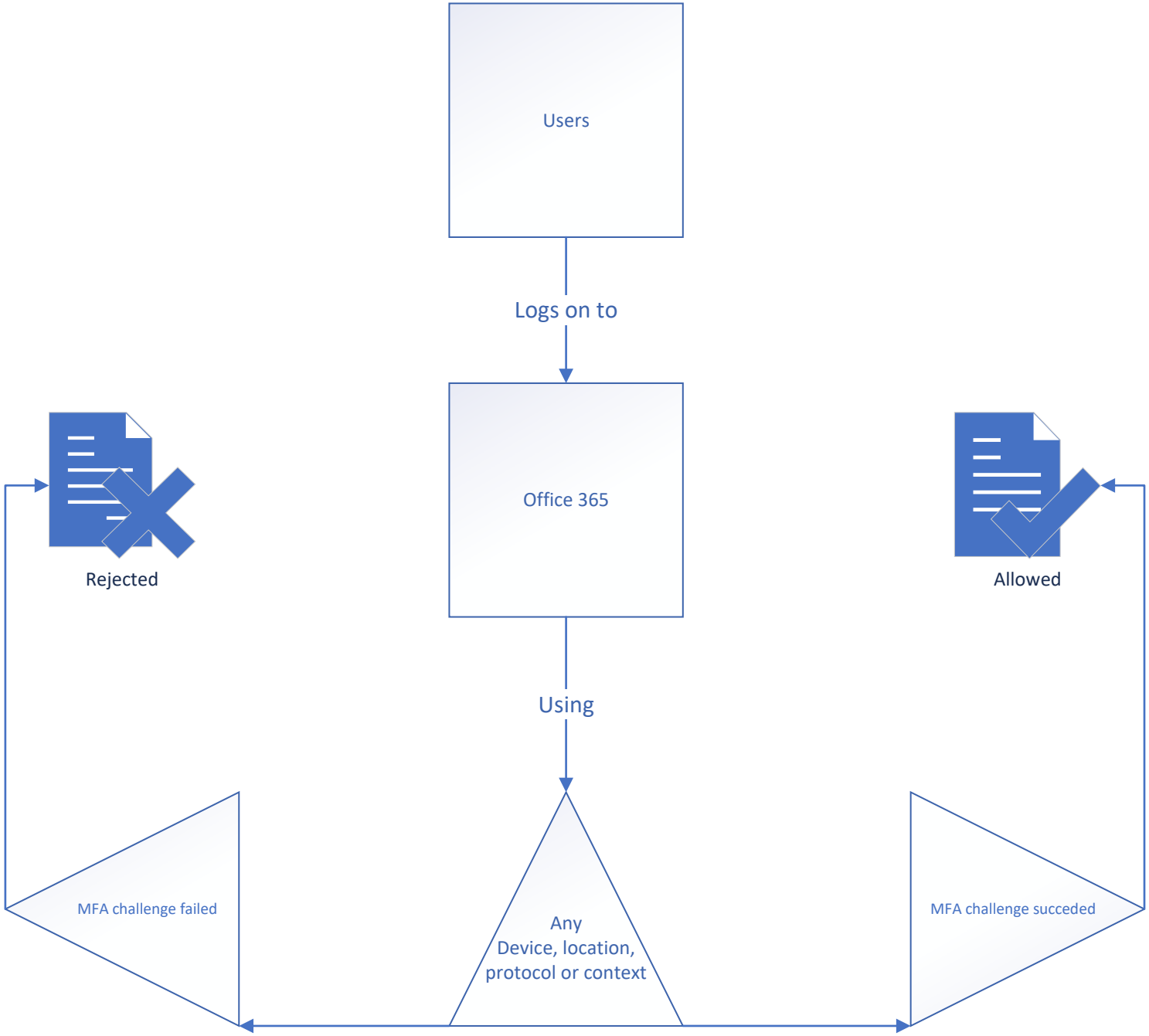
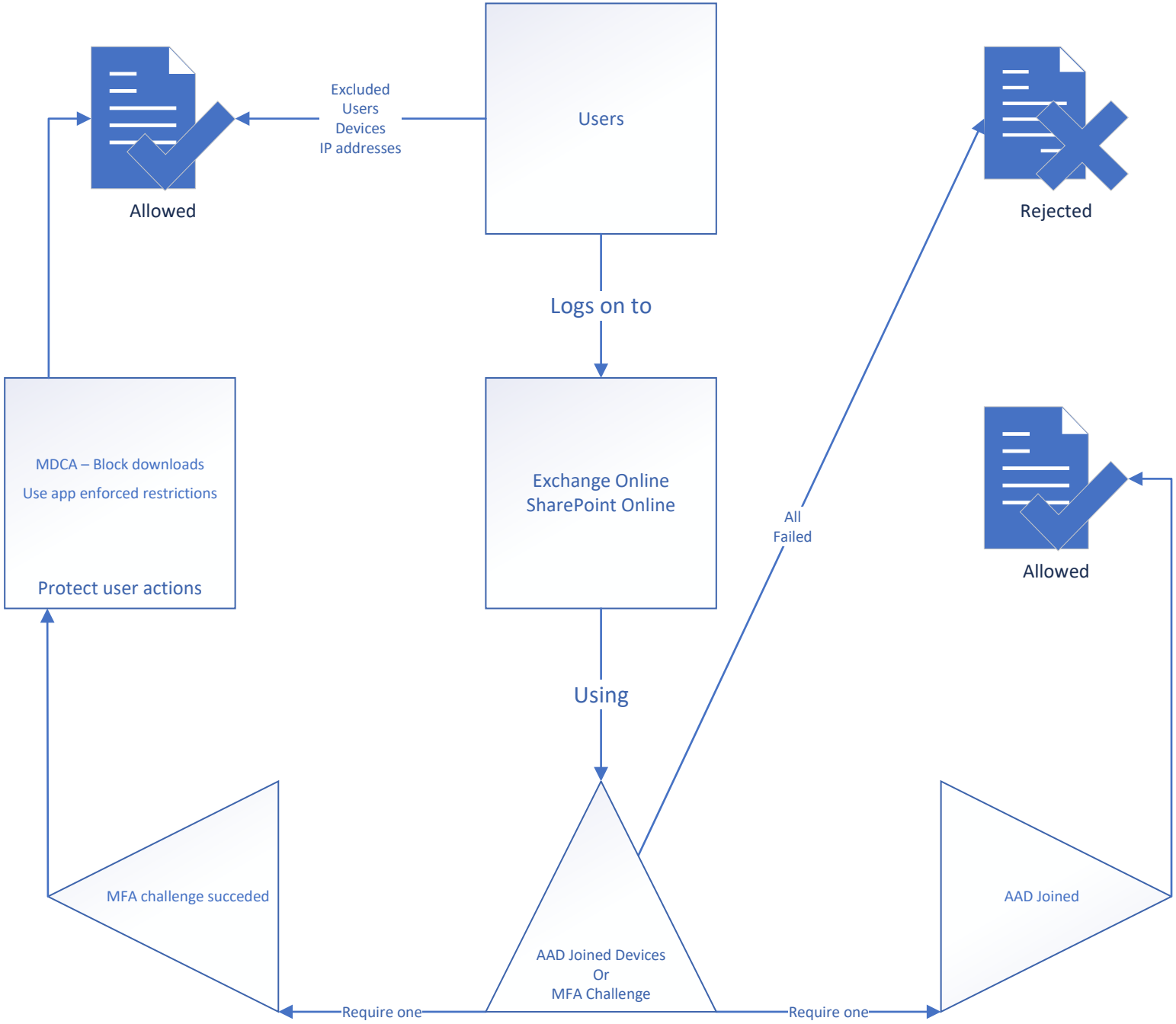
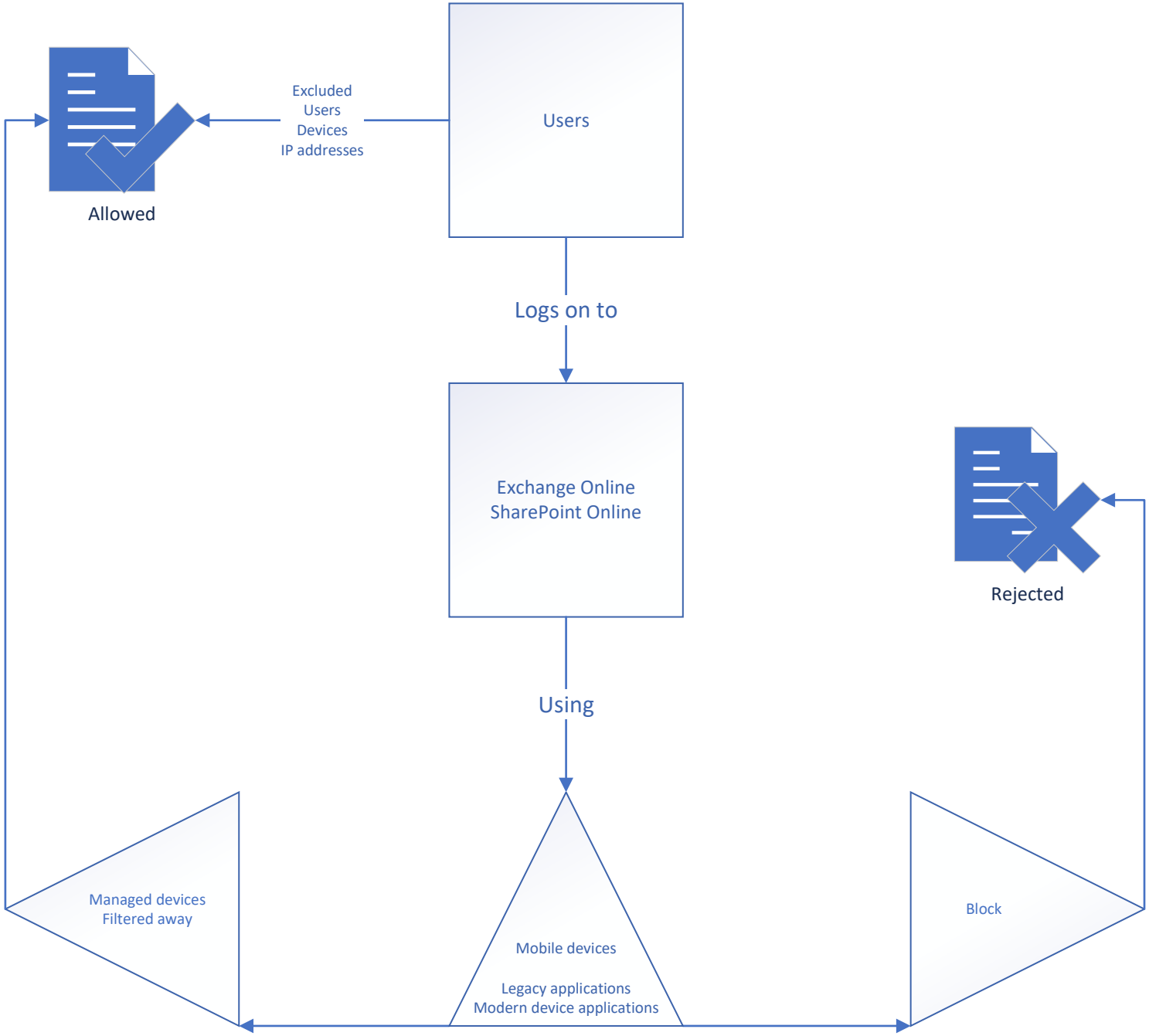
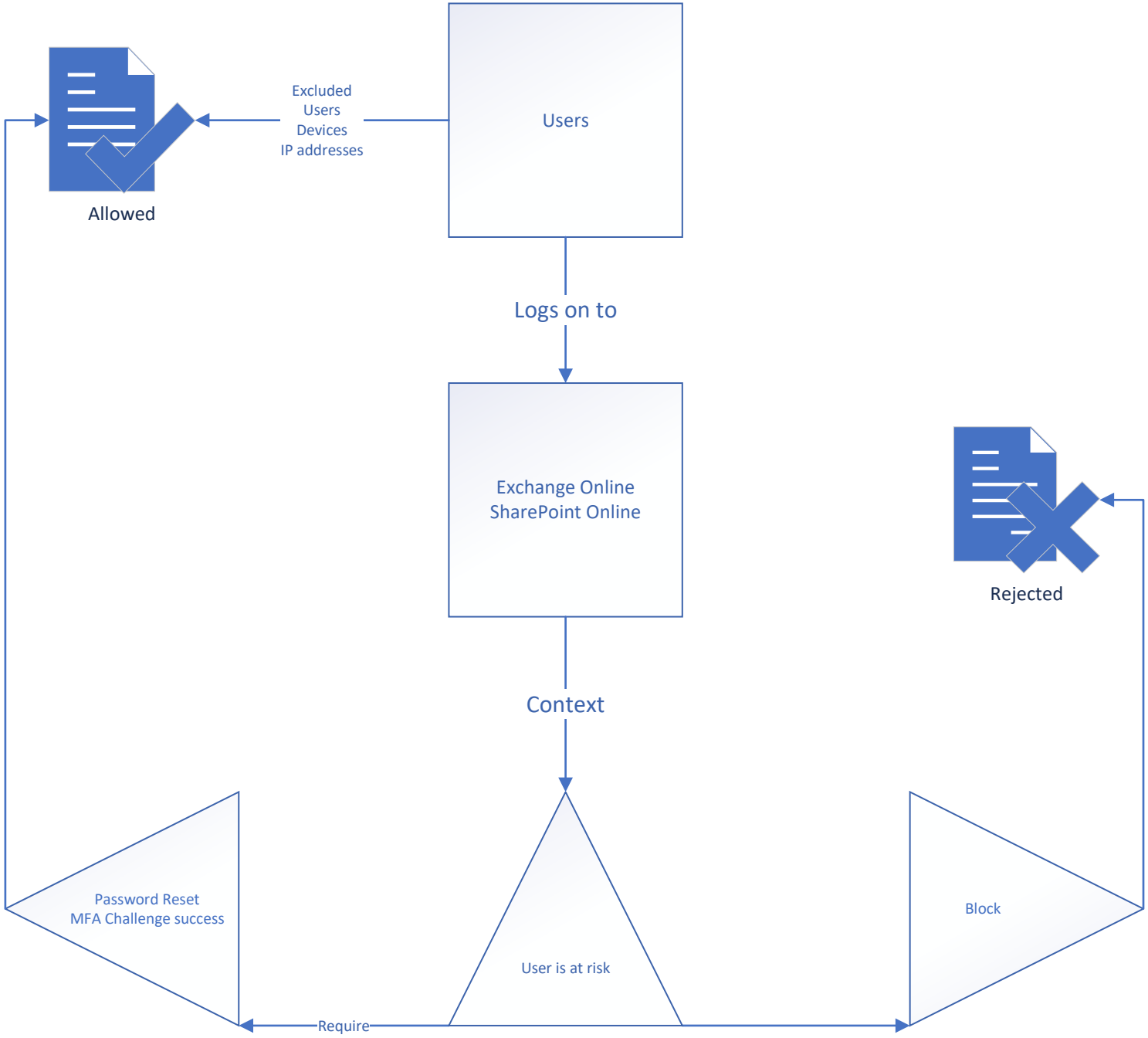

Users
Logs on to
Office 365
Using
Legacy Authentication protocols
Rejected

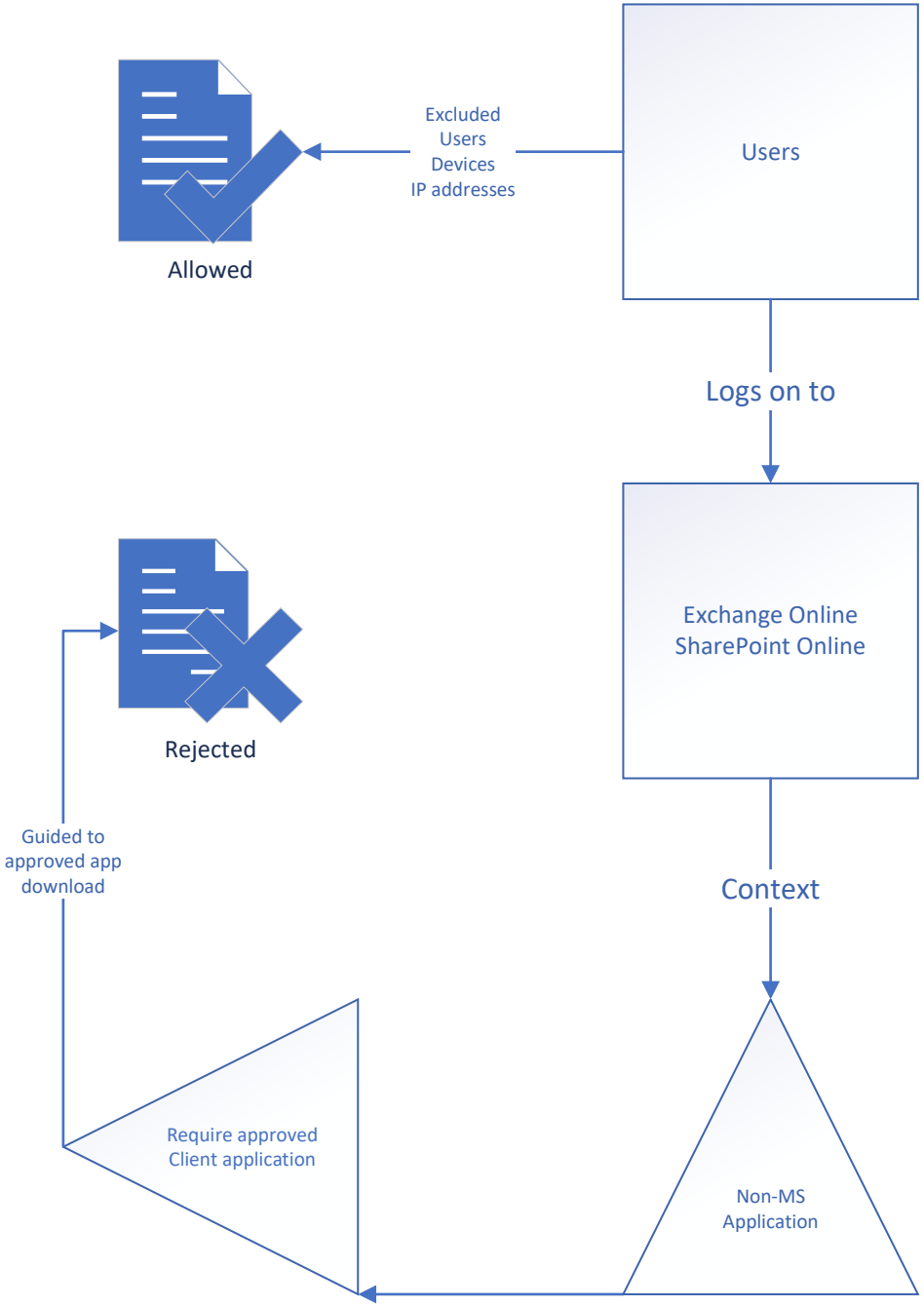

Users
Logs on to
Office 365
Rejected
Allowed
Using
MFA challenge failed
Privileged roles
MFA challenge succeded

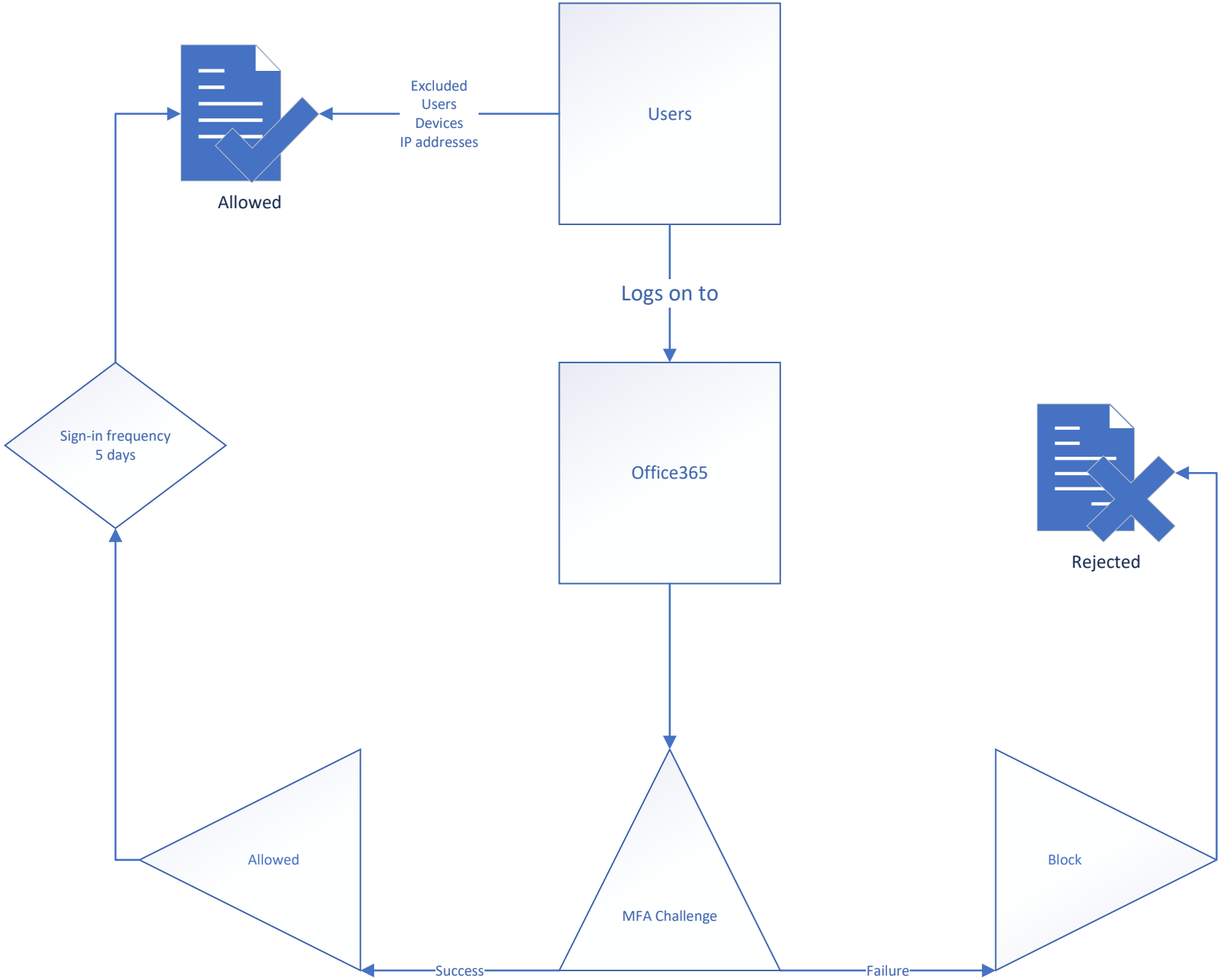

Users
Logs on to
Office 365
Rejected
Allowed
Using
MFA challenge failed
Any
Device, location,
protocol or context
MFA challenge succeded

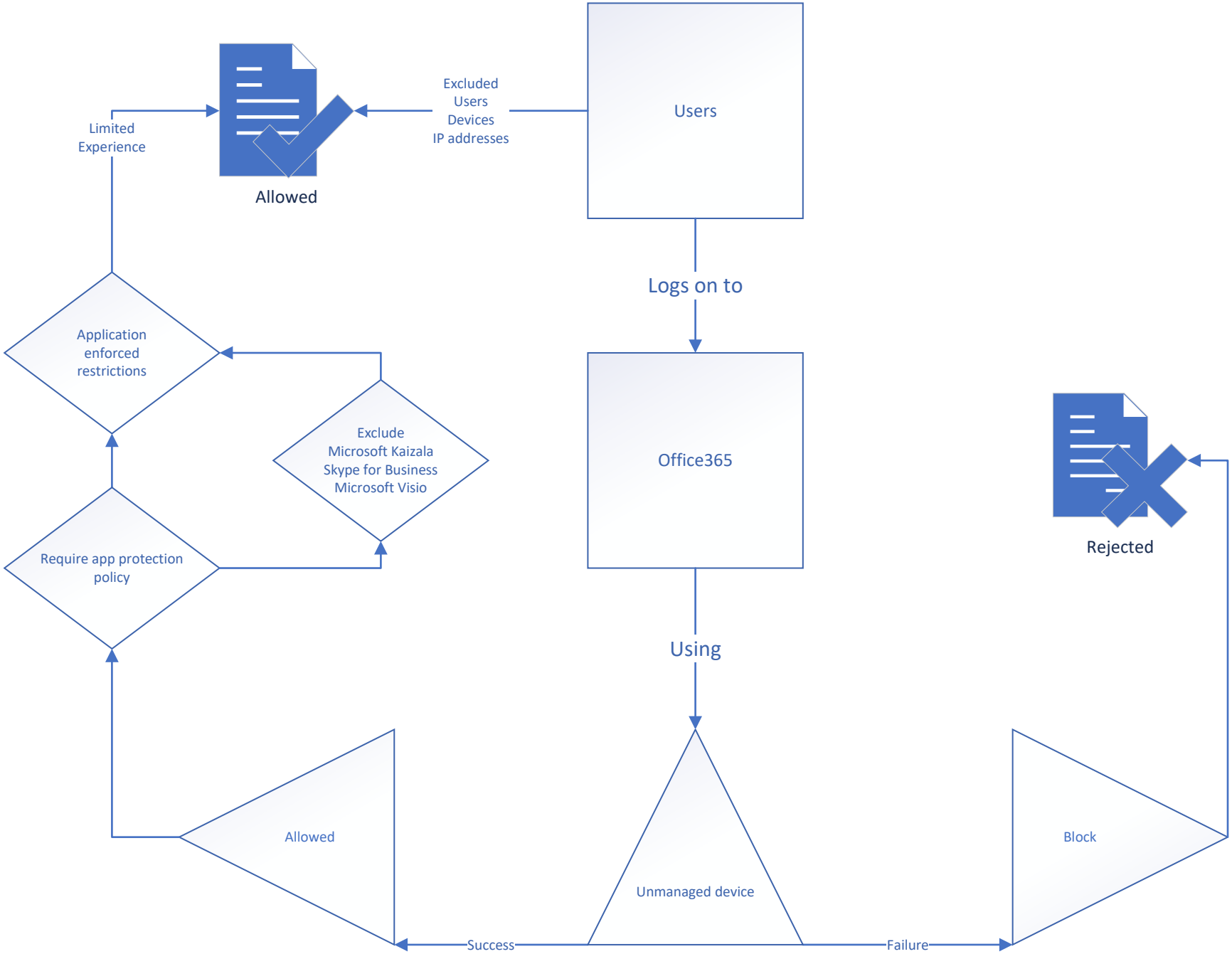

Users
Excluded
Users
Devices
IP addresses
Allowed
Rejected
Logs on to
Exchange Online
SharePoint Online
MDCA – Block downloads
Use app enforced restrictions
Protect user actions
All
Failed
Allowed
Using
MFA challenge succeded
AAD Joined Devices
Or
MFA Challenge
AAD Joined
Require one
Require one

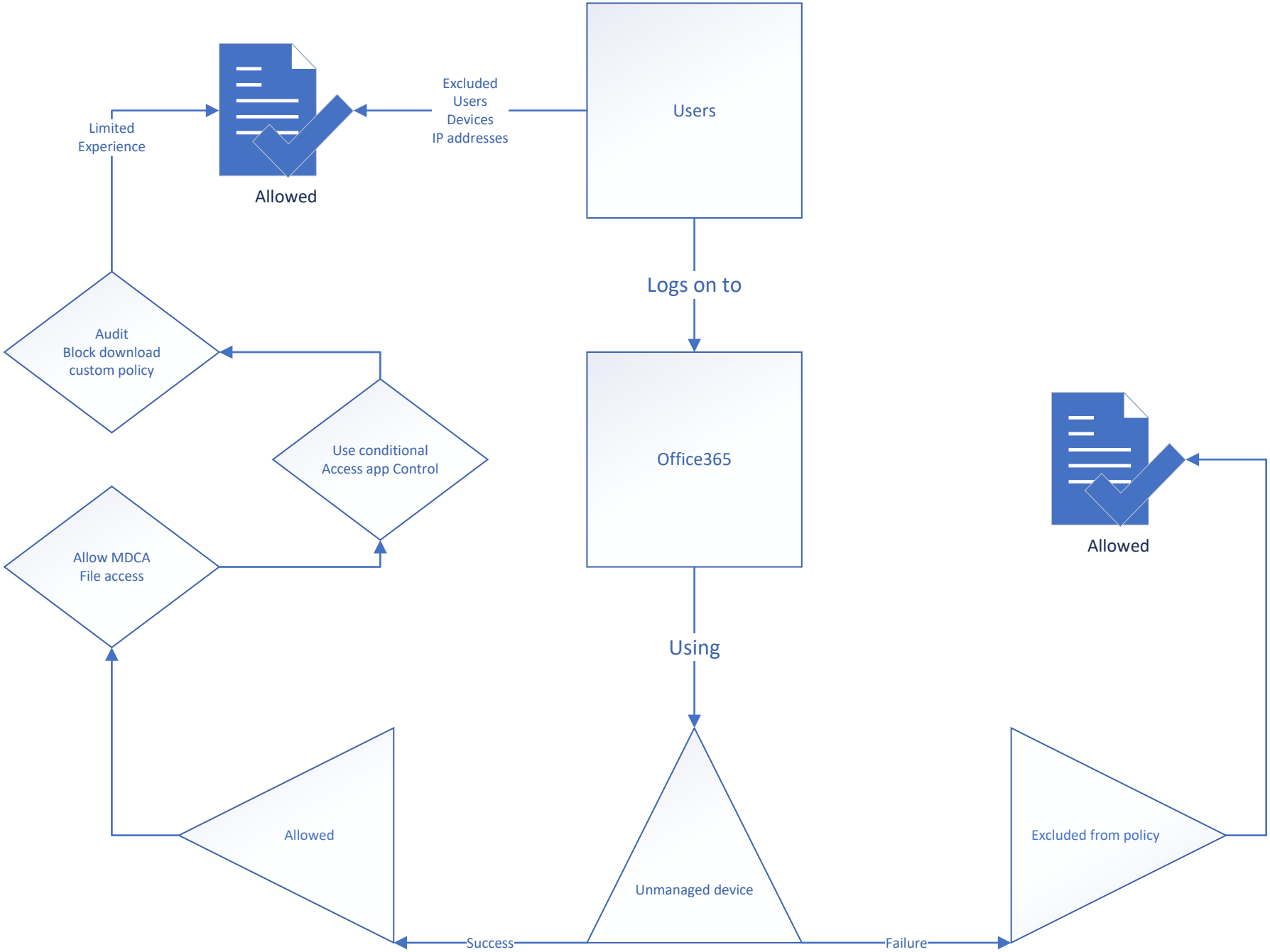

Allowed
Excluded
Users
Devices
IP addresses
Users
Logs on to
Exchange Online
SharePoint Online
Rejected
Using
Managed devices
Filtered away
Mobile devices
Legacy applications
Modern device applications
Block

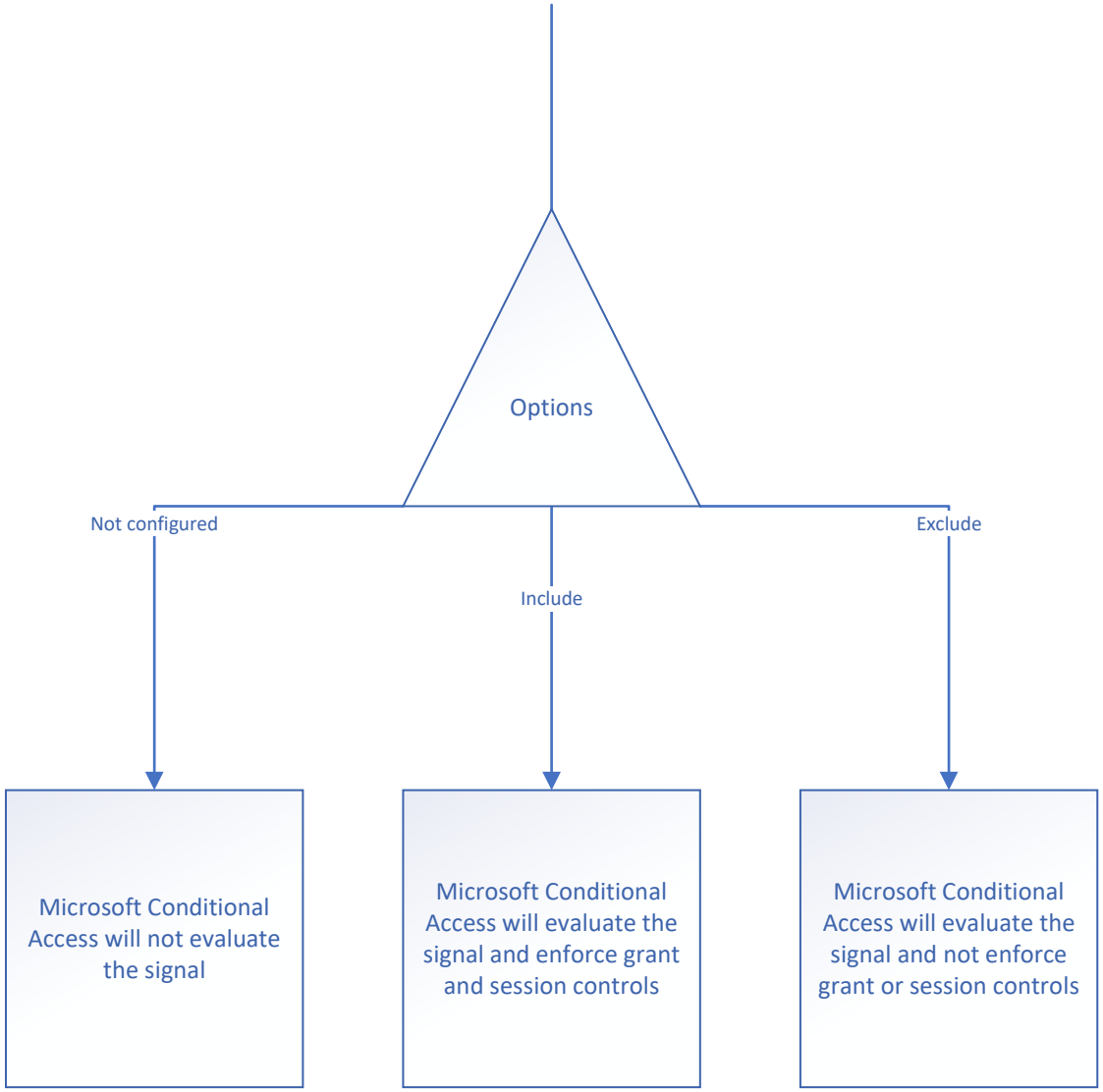

Users
Excluded
Users
Devices
IP addresses
Allowed
Logs on to
Exchange Online
SharePoint Online
Rejected
Context
Password Reset
MFA Challenge success
User is at risk
Block
Require

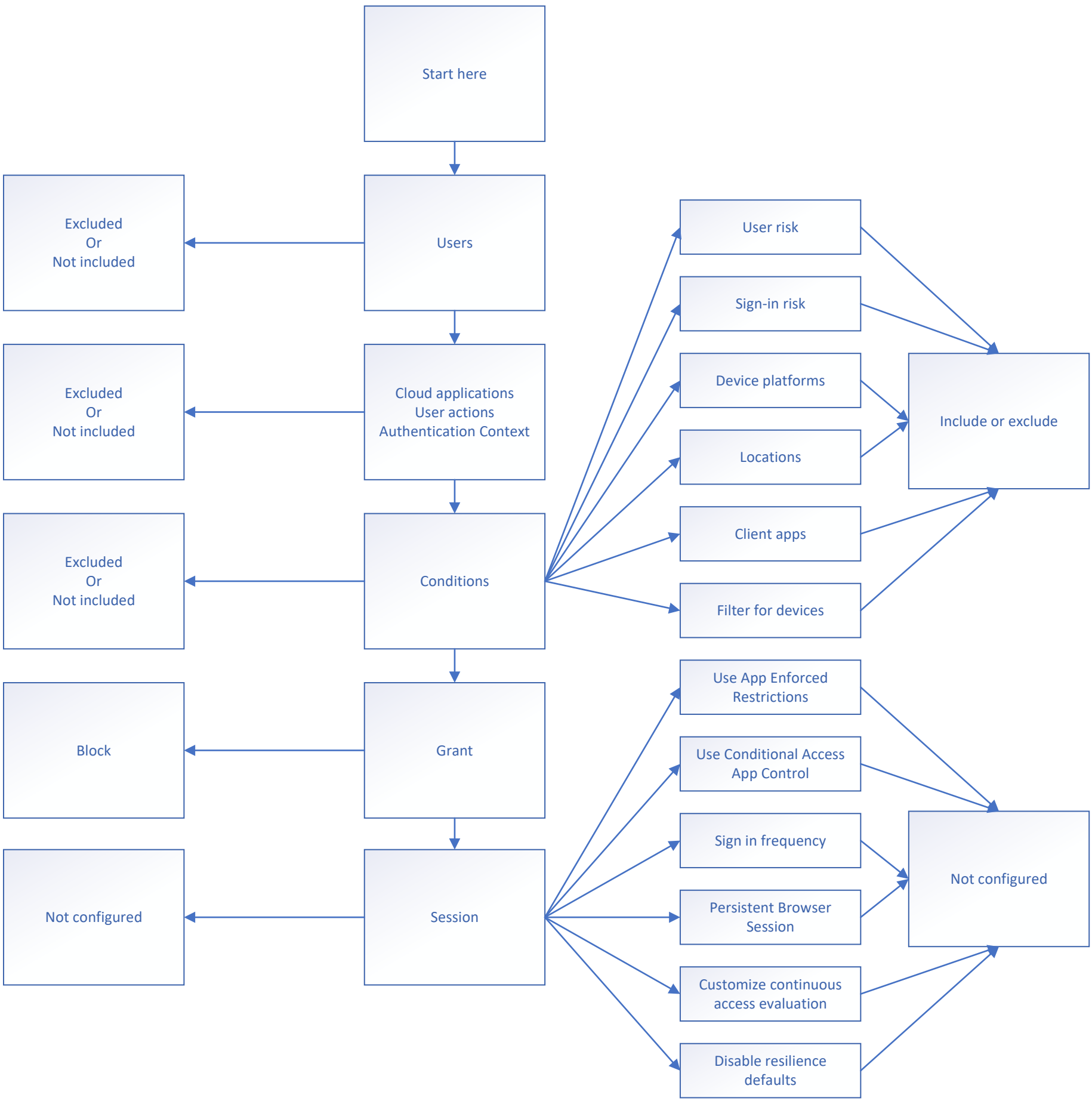

Users
Excluded
Users
Devices
IP addresses
Allowed
Logs on to
Exchange Online
SharePoint Online
Rejected
Guided to
approved app
download
Context
Require approved
Client application
Non-MS
Application

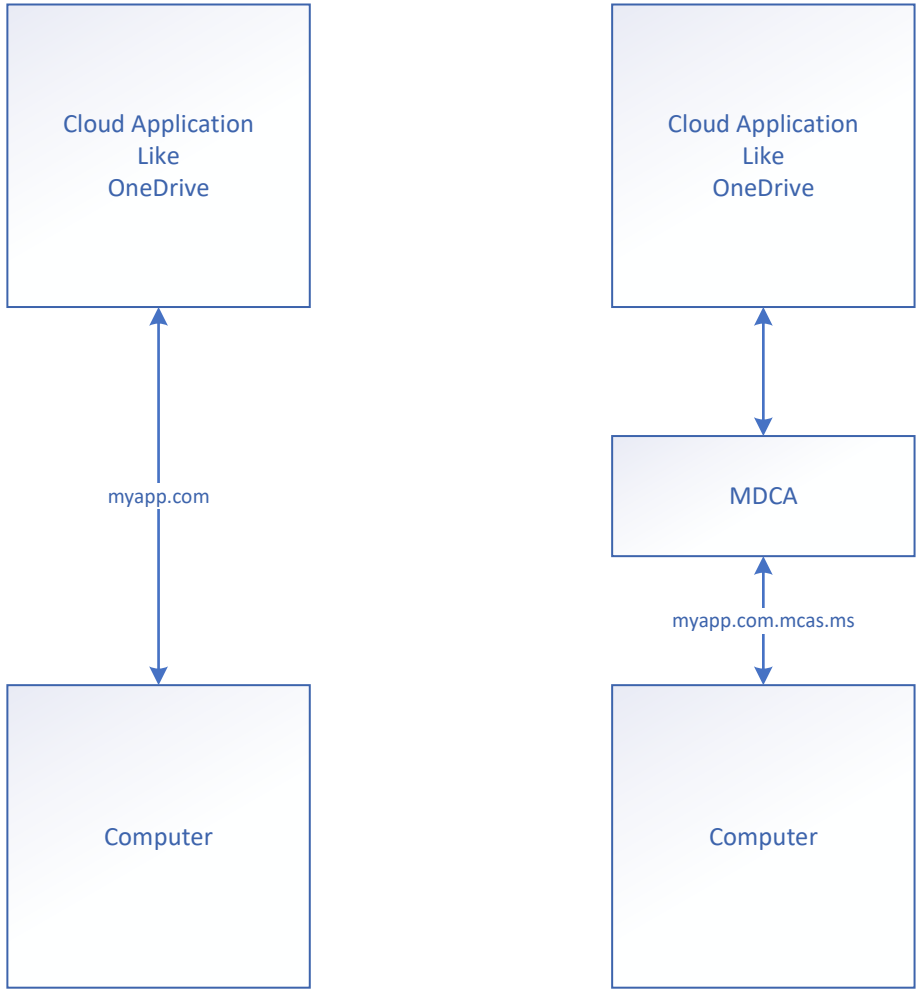

Users
Excluded
Users
Devices
IP addresses
Allowed
Logs on to
Office365
Sign-in frequency
5 days
Rejected
Allowed
MFA Challenge
Block
Success
Failure


Users
Excluded
Users
Devices
IP addresses
Allowed
Limited
Experience
Logs on to
Office365
Application
enforced
restrictions
Exclude
Microsoft Kaizala
Skype for Business
Microsoft Visio
Require app protection
policy
Rejected
Using
Allowed
Unmanaged device
Block
Success
Failure


Users
Excluded
Users
Devices
IP addresses
Allowed
Limited
Experience
Logs on to
Office365
Audit
Block download
custom policy
Use conditional
Access app Control
Allow MDCA
File access
Allowed
Using
Allowed
Unmanaged device
Excluded from policy
Success
Failure


Options
Not configured
Include
Exclude
Microsoft Conditional Access will not evaluate the signal
Microsoft Conditional Access will evaluate the signal and enforce grant and session controls
Microsoft Conditional Access will evaluate the signal and not enforce grant or session controls


Start here
Users
Excluded
Or
Not included
Cloud applications
User actions
Authentication Context
Excluded
Or
Not included
Conditions
Excluded
Or
Not included
Grant
Block
Session
Not configured
User risk
Sign-in risk
Device platforms
Locations
Client apps
Filter for devices
Include or exclude
Use App Enforced Restrictions
Use Conditional Access App Control
Sign in frequency
Persistent Browser Session
Customize continuous access evaluation
Disable resilience defaults
Not configured


Cloud Application
Like
OneDrive
myapp.com
Computer
Cloud Application
Like
OneDrive
MDCA
myapp.com.mcas.ms
Computer

User
Grant / Block
Intune App Protection Policies
Microsoft Defender For Cloud Applications
Protecting data at the app level
End user app use in private context not impacted
Require PIN
Control work-data sharing between apps
Prevent saving to personal device
Integrates with MDM
Block download, cut, copy and print
Require MFA on download of confidential files
Prevent upload of unlabled files
Block potential malware by scanning against MS Threat Intellignce
Monitor For Risk Compliance
Block access based on risk factors