Practical Applications of Conditional Access

McKonly & Asbury

Tax | Assurance | Consulting | Accounting

INTRODUCTIONS

Dave Hammarberg,
CPA , CFE, CISSP, GSEC, MCSE, CISA, CCSFP, CHQP

Partner

Dustin Kinn

Director of Information Technology

FIRM OVERVIEW

McKonly & Asbury is a team of CPAs and Business Advisors serving clients from our offices in Camp Hill, Lancaster, Bloomsburg, and Philadelphia.

We provide **Advisory & Business Consulting**, **Audit & Assurance**, **Entrepreneurial Support & Client Accounting**, **Internal Audit**, **Professional Placement**, **Tax**, and **Technology** services to a variety of industries including:


Affordable Housing


Construction


Employee Benefit Plans


Family-Owned Business


Healthcare


Manufacturing & Distribution


Nonprofits

HAVE YOU HEARD?

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

MODERN THREAT LANDSCAPE

2023 Cybersecurity Statistics (via Forbes, ITRC, FBI)

- 72% increase in data breaches over 2-year period
- Over 343 million people were victims of cyberattacks
- Email Compromise accounts for 35% of malware attacks
- 94% of organizations have reported email security incidents

MODERN THREAT LANDSCAPE

Types of Incidents that most impact organizations

- Ransomware
  - Malicious software designed to block access to data until a sum of money is paid.
- Data Breach
  - Any security incident that results in unauthorized access to confidential information.

MODERN THREAT LANDSCAPE

Professional. Personal.

- Threat Actors are after money
  - Ransomware as an industry is estimated to be worth $14 billion as of 2022.
  - Incidents and scope increased significantly during the pandemic.
  - Average Ransomware attack in 2024 estimated at $2.73 million, up almost $1 million from 2023.

CONDITIONAL ACCESS

Conditional Access is the use of policies and configurations to control access to services and data.

- Uses policies and inputs to determine whether a device or user should be allowed access to an entity.
- Adds additional security over traditional role-based and other access control methods by assessing the device, user, and situation that is requesting access.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Concept of Identity and IAM

- DUO defines Identity Security as safeguarding the digital identities of individuals, devices, and organizations, with three goals in mind:
  - Authentication of a user's identity
  - Authorization of access to appropriate resources
  - Monitoring access activity for vulnerabilities and suspicious activity

IDENTITY AND ACCESS MANAGEMENT (IAM)

- Username and Password is no longer a solely adequate method to secure digital resources.
  - Should be used in conjunction with Conditional Access, Multifactor Authentication, and Zero-Trust methodologies

ZERO TRUST

Zero Trust Architecture

- NIST defines as a cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.
- Eliminates implicit trust and requires continuous verification.

ZERO TRUST

Zero Trust and Conditional Access

- Conditional Access is used to continuously determine things like location, vulnerability, compliance to policies, system device knowledge, session statistics, etc.

COMMON POLICIES

Location-based Policies

- Block access from unknown countries
- Allow access from inside known locations
- Less restrictions from office locations
- Require MFA outside office

COMMON POLICIES

Device-based Policies

- Assess whether device is known to the system
- Allow access to only corporate devices
- Monitor devices for typical usage
- Prevents unauthorized session hijacking

COMMON POLICIES

Risk-based Policies

- Assess risk of account requesting access
- Can utilize device state, IP, and typical vs. atypical behavior to facilitate access
- Used to monitor for suspicious or unauthorized access requests

AZURE CONDITIONAL ACCESS

Main Components used in Azure Policies

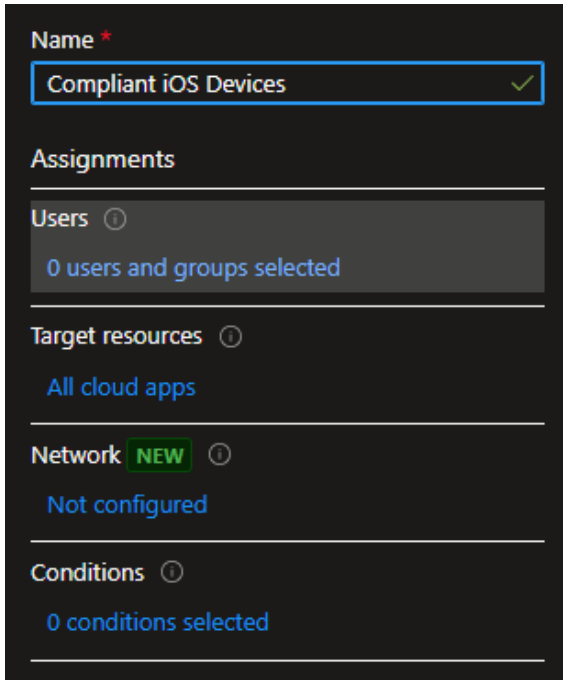
- User Identity – Confirm who is asking
- Device Security – Validate if the request is expected behavior
- Location – Determine if request is coming from an expected, known, or explainable location
- What access is being requested

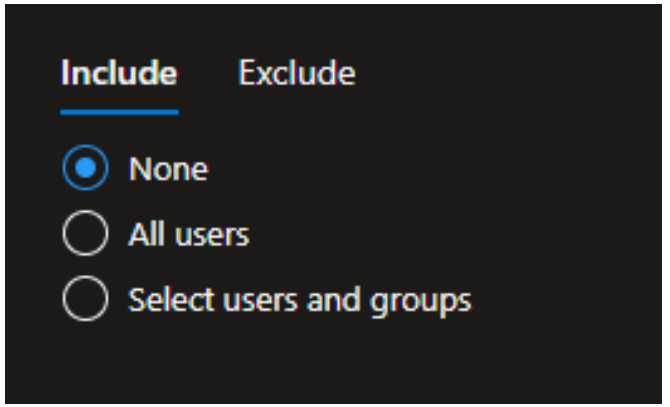
AZURE CONDITIONAL ACCESS

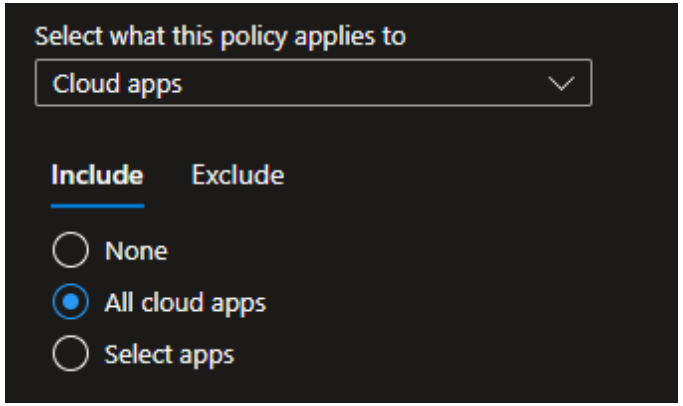
Example Policy – Compliant Devices

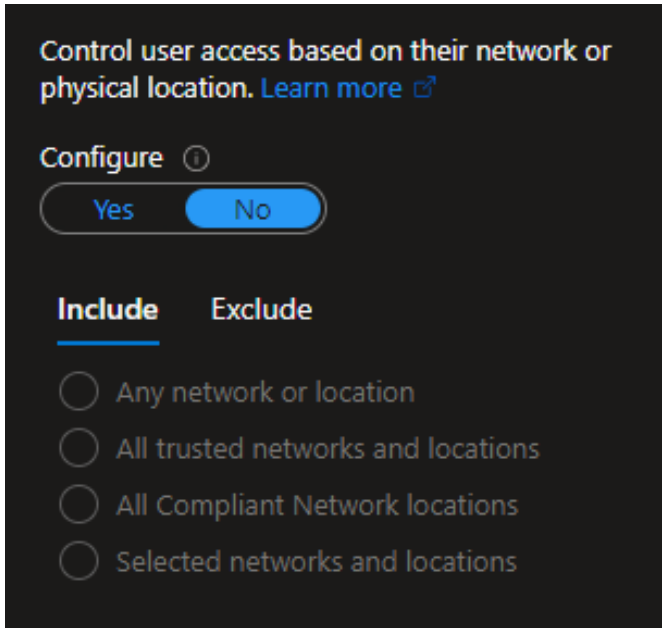
- Policy will require devices be marked as compliant inside Azure before being allowed to access Azure resources
- Scope Apple iOS Devices
- Target Office 365 Mobile Apps

ASSIGNMENTS

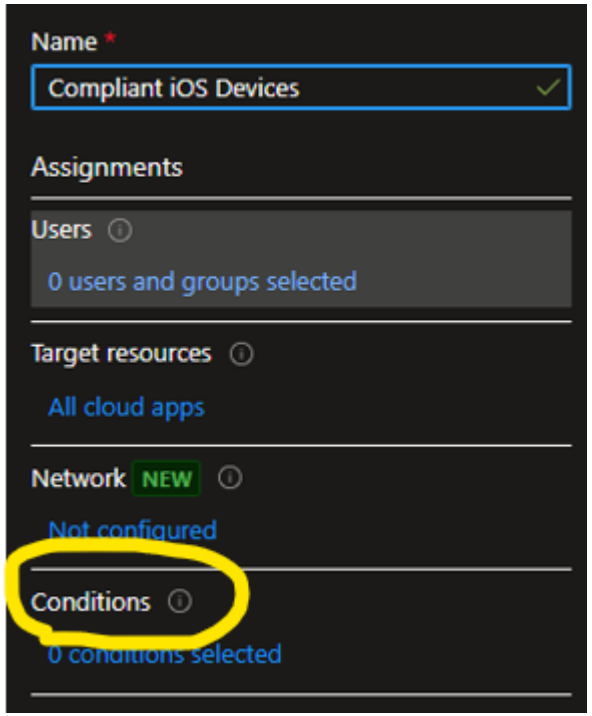


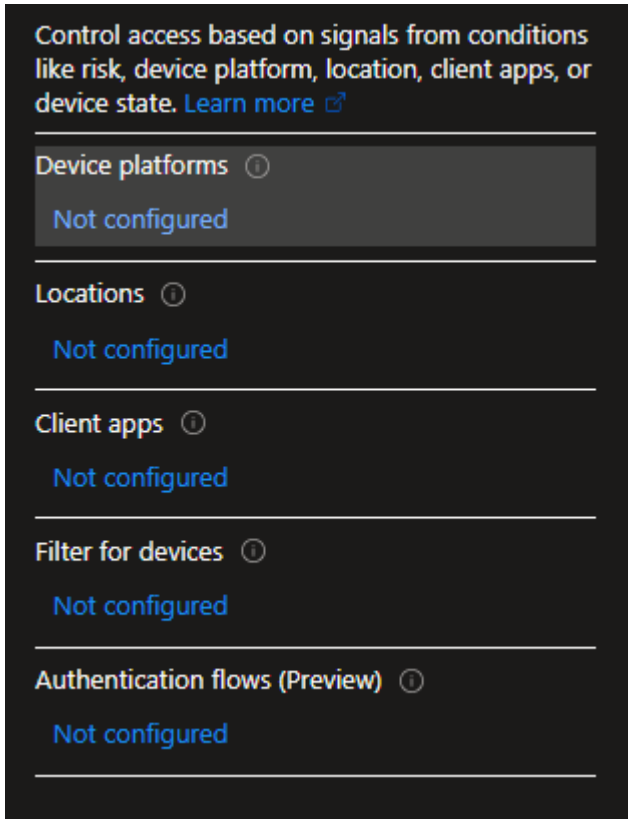


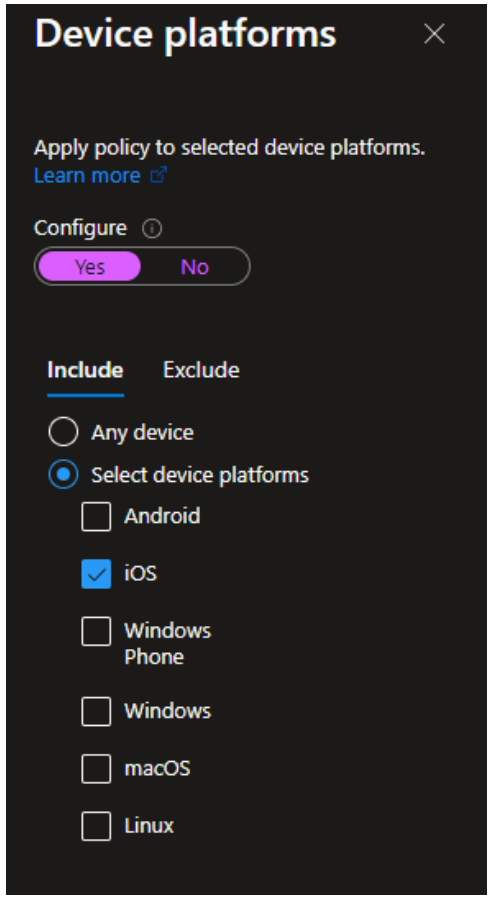




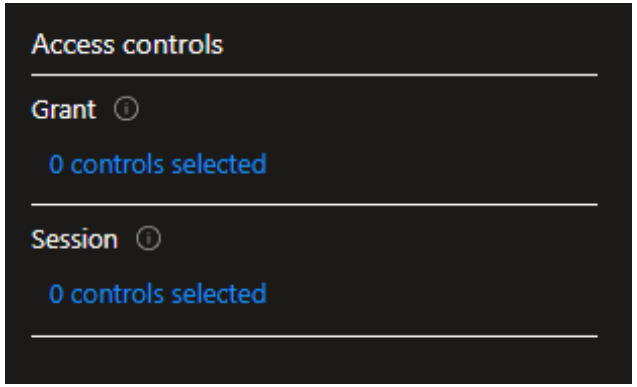
ASSIGNMENTS

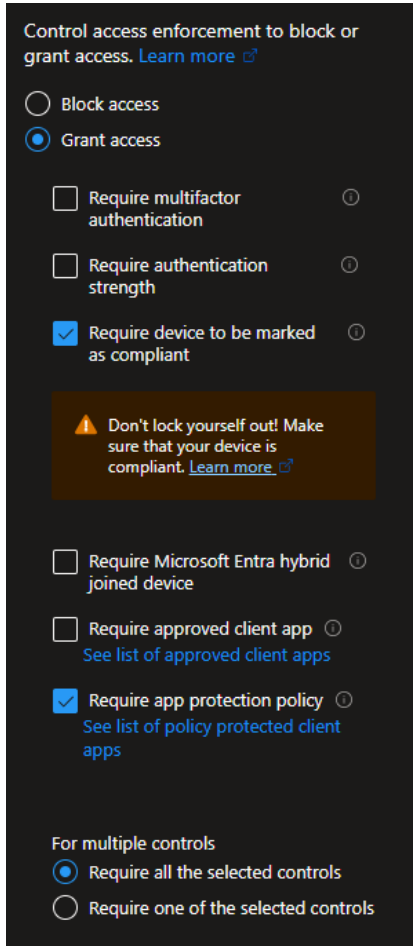


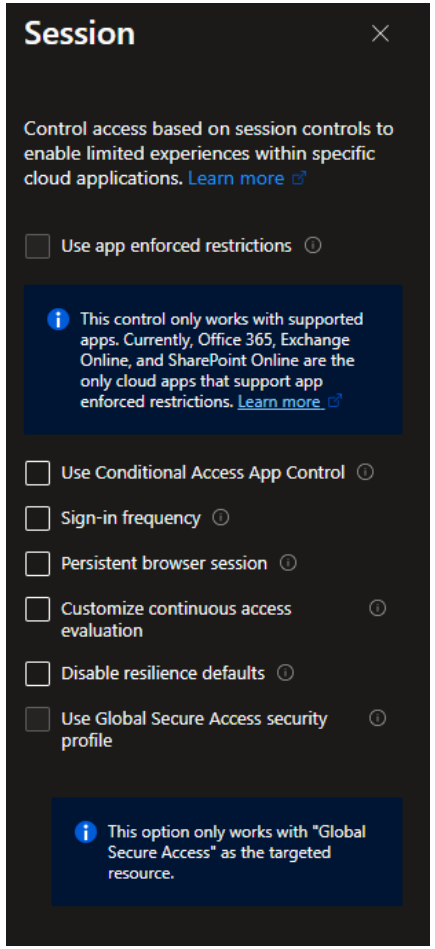




ACCESS CONTROLS



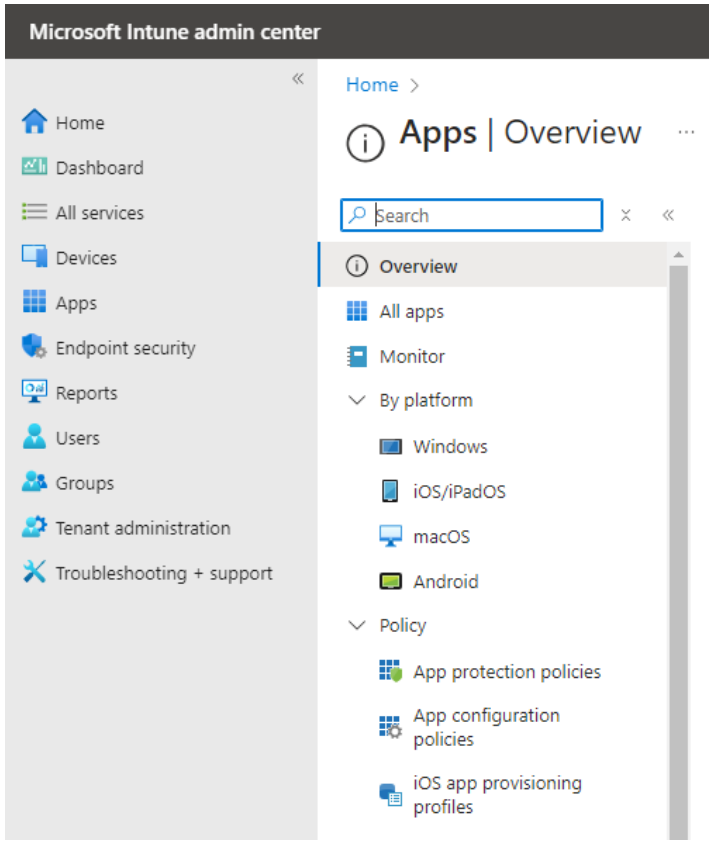


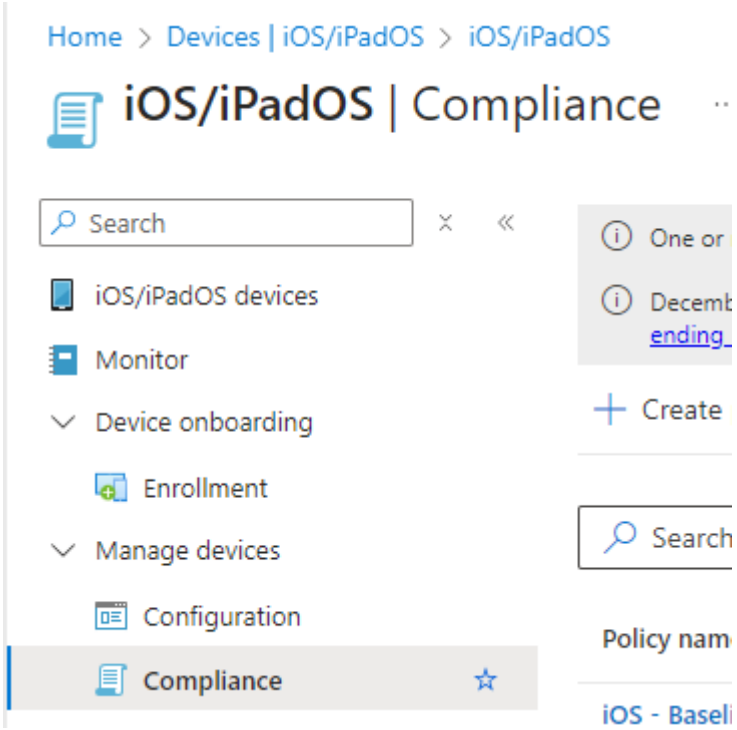


TESTING AND DEPLOYING

- Report-only mode
  - Policy evaluates but does not enforce
  - Logs results in the sign-in log details
- Recommend assignment to test group before turning on for everyone
  - Can validate functionality before deploying across organization

REQUIRED INTUNE POLICIES





McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

AZURE CONDITIONAL ACCESS

Summary

- Conditional Access Policy Created
  - User and device targets assigned
  - Application targets set
  - Condition for access defined
- Intune Policies Created
  - Compliance Policy
  - App Protection Policy

PROTECTION

Examples of typical Conditional Access Policy Targets

- Microsoft/Office 365 Cloud Applications
- Cloud Services able to utilize Office 365/Azure Authentication
- Mobile Devices
- Remote Users
- Frequent Travelers

BENEFITS

- Enhanced Security
- Compliance with frameworks and regulations
- Easier User Experience
- Improved Administration

CONSIDERATIONS

- Policies can quickly become complex in scope
  - Separate policies for each objective when possible
- Balance usability with security
  - Make sure to understand what is being protected and against what
- Scalability
  - Avoid policies that target one user or device
  - Make sure policies are not conflicting

BEST PRACTICES

- Consistent Review of Policies
  - Recommend Monthly review with at least annual third-party assessment
  - Watch for new policy options and understand how they impact environment
- Training and Awareness
  - Explain to users what the policies do, what they protect, and what they prevent
- Monitor logs for unusual activity and potential threats
  - Sign-in logs on Azure show what Conditional Access policies tripped for each event, recommend regular review and where possible logging to an event and incident management system (SEIM)

Q&A

Questions?

CONTACT INFORMATION

Dave Hammarberg,
CPA, CFE, CISSP, GSEC, MCSE, CISA, CCSFP, CHQP

Partner

dhammarberg@macpas.com

717-972-5723

Dustin Kinn

Director of Information Technology

dkinn@macpas.com

717-972-5815

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

UPCOMING EVENTS

OCTOBER 24 SEMINAR

Free Nonprofit Seminar

October 24, 2024
8:30 am - 12 pm

The HUB at Mulberry Mill
160 W. 6th Street
Bloomsburg, PA 17815

presented by:

McKONLY & ASBURY

Community
STRATEGIES GROUP

Register Today!

OCTOBER 31 WEBINAR

Register Today!

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

Visit us online at **www.macpas.com** for more information.

NOVEMBER 7 SEMINAR

Affordable Housing Seminar
Featuring A.J. Johnson

November 7, 2024
9:30 am - 3:30 pm

Giant Community Center
3301 Trindle Road
Camp Hill, PA 17011

Register Today!

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

Visit us online at **www.macpas.com** for more information.