Protect your data at the front door

Enterprise Mobility + Security (EMS)
conditional access
Contents

1. Safeguard resources with advanced risk-based conditional access

2. Breaking down EMS conditional access
   - Application parameters
   - User parameters
   - Location parameters
   - A sample conditional access scenario

3. Device-based conditional access
   - Device compliance
   - Adding Lookout to provide additional mobile endpoint security
   - Device-based conditional access to on-premises resources

4. Risk classification
   - Leaked credentials
   - Impossible travel or atypical locations
   - Sign-ins from potentially infected devices
   - Sign-ins from anonymous IP addresses
   - Sign-ins from IP addresses with suspicious activity

5. Beyond access control
   - For more information
Safeguard resources with advanced risk-based conditional access

The adoption of mobility and cloud services has changed the way business users interact with their devices, apps, and corporate data, increasing the options for users to connect and be productive at any time.

Users expect the freedom to access their corporate email and documents from anywhere on any device—with a seamless and modern experience. Mobile productivity requires innovative tools that flex and flow to give end users the best possible experience across their devices, while protecting corporate data in a threat landscape that is increasingly complex and sophisticated.

Conditional access from Enterprise Mobility + Security (EMS) harnesses the power of Azure Active Directory Premium and Microsoft Intune to provide the control necessary to help keep corporate data secure, while still enabling people to do their best work from any device.

With conditional access, you can define policies that limit access to your corporate data based on location, device state, user profile, and application sensitivity. These policies can adapt to real-time conditions based on perceived risks. For example, our machine learning-based Azure AD Identity Protection, which leverages billions of signals daily, can detect suspicious behavior and trigger controls to allow or block user access. Policies can also challenge users with Multi-Factor Authentication, device enrollment, or password change to help ensure that only trusted users on compliant devices can access sensitive corporate data.

Breaking down EMS conditional access

Let's explore the conditional parameters that can be used at the application, user, and location layers.

Figure 1. EMS lets you define policies that tailor access to corporate data and applications based on location, device state, user profile, and application sensitivity.
Application parameters

While you may want to allow easy access to some useful cloud apps, you likely want to use more rigor for apps that store highly sensitive information. When you consider how much application scenarios can vary, it’s clear you need more than a one-size-fits-all approach to app-level control. That’s why our application-based conditional access allows you to choose which policies to apply to which apps.

You can set a policy that allows access to apps based on criteria you define. For example, you can require Multi-Factor Authentication every time an app is accessed. Or you can block access from suspicious or unknown locations. Policies can also apply to virtually any cloud (SaaS) or on-premises app protected by Azure Active Directory, whether the client is rich, mobile, or browser-based.

User parameters

Azure Active Directory Premium advanced identity and access management is the foundation for all conditional access capabilities. You can choose which conditional access policies apply to which groups of users. You can specify multiple conditions (based on location, application, device, and risk) for all users or for individual security groups. You can also specifically exclude groups from conditional access policies.

Location parameters

Location-based conditions can limit access to a defined set of trusted IP addresses. You define what happens next when a user attempts to access corporate assets from an unknown network. For example, policy controls can challenge the user with Multi-Factor Authentication (MFA) or block access entirely. You can also define which user groups these polices will affect.

A sample conditional access scenario

The scenario illustrated below shows how conditional access policy works at the user, location, and application layers.
Figure 2. Because the app Julia is trying to use provides access to highly sensitive data, IT has applied a location-based conditional access policy that denies access when users, including those in the marketing security group, are working from an untrusted location.

To explore additional conditional access scenarios, visit our conditional access web experience.

Device-based conditional access

Typical employees connect multiple devices to their corporate network, and they don’t always connect from their own mobile device or PC. Perhaps an employee uses her daughter’s iPad in a pinch, signs in from a friend’s laptop, or uses a hotel kiosk to connect. You might be comfortable allowing access in some cases, but in others you may want to limit access to certain employees, to specific data, or to devices that are known and compliant. EMS helps you do this.

Device compliance

Device compliance policies make sure devices attempting to access your data or sensitive apps first meet your specific requirements or standards. Administrators can set policies to enforce device enrollment, domain join, strong passwords, and encryption. Policies can also require that device operating systems and apps be up-to-date with the latest patches before granting full access.

You can use compliance policy settings in Microsoft Intune to evaluate the compliance of employee devices against a set of rules you create. When devices don’t meet the conditions set in the policies, Intune guides the end user though enrolling the device (if it’s not already enrolled) and fixing the compliance issue.
When you combine a device compliance policy with conditional access, only authorized users will gain access, and only from compliant devices. Since both policies are applied at the user level, EMS examines any device the user employs to access services (e.g., corporate-issued, personal, daughter’s iPad, friend’s laptop, or hotel kiosk) to ensure it’s compliant. Figure 3 illustrates the combination of conditional access and device compliance policies.

Figure 3. In this scenario, IT has applied policies that require devices to be enrolled before the user can access and open files stored on OneDrive for Business.

Adding Lookout to provide additional mobile endpoint security

The deep integration of Lookout Mobile Endpoint Security with EMS gives real-time visibility into advanced mobile threats and app data leakage. Lookout provides visibility across all three mobile risk vectors: app-based risks (such as malware), network-based risks (such as man-in-the-middle attacks), and OS-based risks (such as malicious OS compromise). The integration between Lookout and EMS makes it easy to apply this threat intelligence to your conditional access policies. If Lookout identifies a device as non-compliant, Lookout guides the user through resolving the issue before they can gain access.

Note: Lookout licenses must be purchased separately from EMS.
Device-based conditional access to on-premises resources

EMS conditional access capabilities help secure access to both cloud and on-premises resources. They also simplify management for organizations that use Azure Active Directory Application Proxy to enable secured access to on-premises applications without VPNs, DMZs, or on-premises reverse proxies. Best of all, you can do all of this without installing or maintaining additional on-premises infrastructure or opening your company firewall to route traffic through it.

Since our customers often manage broad and complex networks, we have partnered with popular network access providers such as Cisco ISE, Aruba ClearPass, and Citrix NetScaler to extend Intune’s conditional access capabilities. Partner network providers can require checks for Intune-managed and compliant devices before allowing user access through either wireless or virtual private networks. Extending device compliance policies to network providers enhances your ability to ensure that only managed and compliant devices can connect to your on-premises corporate network.

Risk classification

In addition to addressing user- or device-based vulnerabilities, it’s important to consider the rest of the threat landscape, which can be highly complex.

Even the most sophisticated attacks leave behind traces that can form detectable patterns. Every month Microsoft processes a tremendous volume of these signals. In addition, we update more than 1 billion PCs, service more than 450 billion consumer and enterprise authentications, and analyze more than 200 billion emails for malware and malicious websites. Our threat intelligence systems see just about every kind of attack there is and we push all that data directly into our Microsoft Intelligent Security Graph.

The Intelligent Security Graph pulls together telemetry and signals from the hundreds of cloud services that Microsoft operates, extensive and ongoing research that identifies emerging attack vectors and malware, as well as data from partnerships with industry leaders and law enforcement organizations. We
apply our machine learning and data analytics to identify anomalous and suspicious activities that characterize advanced and persistent attacks. The graph makes it possible for us to deliver recommendations and automated actions to help prevent attacks and to counter them. It achieves this by calculating and assigning a risk level (low, medium or high) to every sign-in activity and user account based on the gathered data. We also assign a risk score to possible configuration vulnerabilities, such as administrators with weak authentication options, or the absences of initial an MFA configuration for end-users.

Based on this risk classification, conditional access policies can block access for high-risk users or for high risk sign-ins. For medium or low risk users and events, policies can require additional authentication steps, such as multi-factor authentication, password reset or device enrollment, before granting access.

The most common events that affect the risk calculation are described below.

**Leaked credentials**

Microsoft security researchers search for credentials that have been posted on the dark web, which usually appear in plain text. Machine learning algorithms compare these credentials with Azure Active Directory credentials and report any match as “leaked credentials.”

**Impossible travel or atypical locations**

Machine intelligence detects when two sign-ins originate from different geographic locations within a window of time too short to accommodate travel from one to the other. This is a pretty good indicator that a bad actor succeeded in logging on.

Machine intelligence also flags sign-ins at atypical locations by comparing them against past sign-ins of every user. Sign-ins from familiar devices or sign-ins from or near familiar locations will pass.

**Sign-ins from potentially infected devices**

The Microsoft Intelligent Security Graph maintains a list of IP addresses known to have been in contact with a bot server. Devices that attempt to contact resources from these IP addresses are possibly infected with malware and are therefore flagged.

**Sign-ins from anonymous IP addresses**

People who want to hide their device’s IP address, often with malicious intent, frequently use anonymous proxy IP addresses. A successful sign in from an anonymous IP address is flagged as a risky event. If the risk score is medium, a risk-based conditional access policy can require MFA as an additional proof of identity.
Sign-ins from IP addresses with suspicious activity

Multiple failed sign-in attempts that occur over a short period of time, across multiple user accounts, and originate from a single IP address, also trigger a risk event. Traffic patterns that match those of IP addresses used by attackers are a strong indication that accounts are either already compromised or will be very soon, although the traffic pattern may also originate from an IP address shared with multiple devices via a router or similar device.

Beyond access control

While conditional access policies and machine intelligence help protect your data “at the front door,” a holistic security strategy requires additional measures. For example, you still need to protect against successful invasions and legitimate users who may compromise data, whether inadvertently or maliciously. EMS and Office 365 offer features that help you manage which cloud services people can use to view, edit, and store sensitive data, and make it possible to encrypt and track data shared outside your organization. For more information, visit the links listed below.

For more information

Websites

- EMS website
- Conditional access web experience
- Enterprise mobility and security blog

Documents

- Protect Office 365 company data with Intune
- Conditional access in Azure Active Directory

© 2017 Microsoft Corporation. All rights reserved. This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.