DUO for...

Microsoft

Office365, Azure and Windows

Companies are moving their on-premises Microsoft applications to the Microsoft cloud. As they migrate, they must move their security alongside their application stack. Duo helps customers stay secure during this migration, protecting both on-premises and cloud-based Microsoft applications by ensuring that only the right users using secure devices can connect to the right applications - this is the core principle of Duo's Trusted Access platform.

THE CHALLENGE:

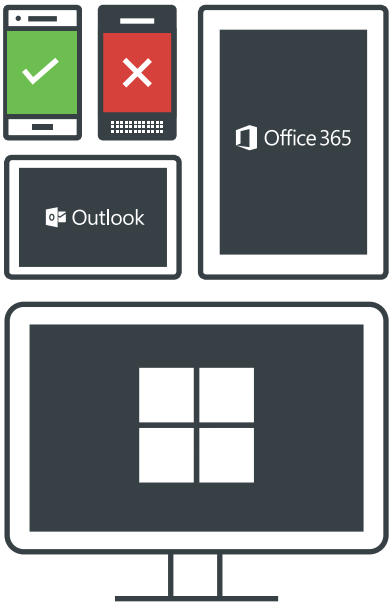
Cloud Migration and a Single Set of Credentials Pose Security Risk

Microsoft offers a number of powerful productivity tools like the Microsoft Office Suite and Windows Desktop. When coupled with Microsoft Active Directory, these tools become even more powerful and easy to use.

Active Directory is truly the core of your network - a single set of credentials can allow your users to log into all of your applications. While this optimizes productivity with a single username and password to access all applications, it also increases the risk of breach. Additionally, as organizations move to Azure Active Directory, they want to maintain the same best-of-breed security solutions they've become accustomed to using.

Socially engineered campaigns, like phishing attacks, are incredibly efficient in fooling end users into giving up their credentials. With the right set of credentials, hackers can gain privileged access to sensitive corporate emails and documents available in Office 365; critical applications and data through remote desktop sessions; and much more.

This is further complicated as companies move their applications to the Microsoft cloud. Traditional security appliances cannot easily protect both on-premises and cloud workloads, leaving many companies vulnerable to attack.



THE SOLUTION:

Duo Secures Access to All Microsoft Applications

With Duo's Trusted Access platform, you can easily protect your users, devices and apps within your Microsoft environment. Duo provides powerful two-factor authentication, device insight and access control policies for popular Microsoft applications like Outlook Web Access, Office 365 and Remote Desktop. Duo's solution also integrates with both on-premises and Azure Active Directory to facilitate role-based access for all of your employees. It even offers a native integration with Azure AD Conditional Access so any application connected with Azure AD can be automatically protected with Duo.

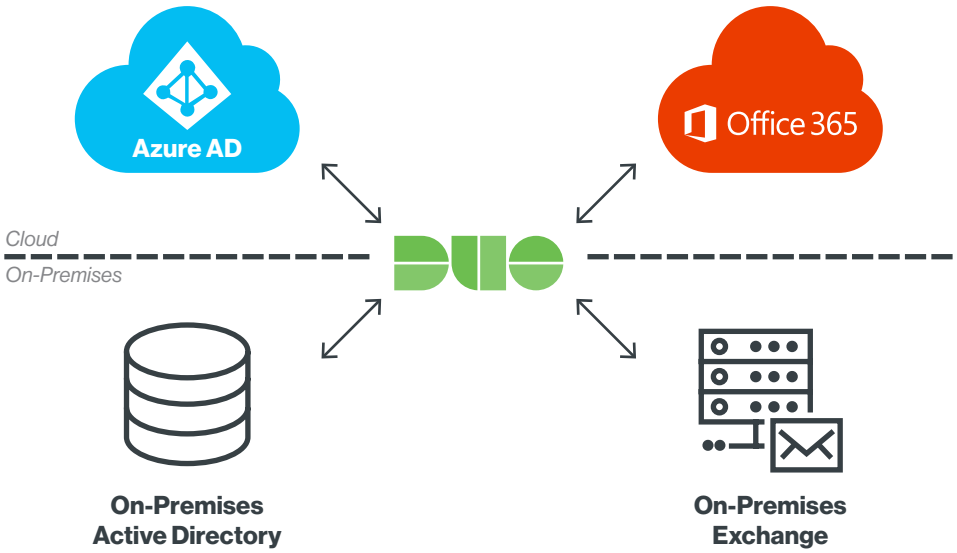
The Use Cases:

Securing Email

Companies are replacing their on-premises Exchange servers with cloud-based email through Office 365. But this migration takes time, and most organizations deploy Office 365 incrementally. This means companies must figure out how to secure both their on-premises and cloud email infrastructure at the same time. Duo secures access to both Outlook Web App and Office 365 so companies can safely migrate to the Microsoft cloud.

Duo and Microsoft have partnered to provide native multi-factor authentication for companies using Office 365 and Azure Active Directory. This allows joint customers to use Duo to securing access to their Office 365 workloads and other Microsoft Azure applications. This results in more granular security controls and a better user experience. Administrators can configure this directly within their Azure Active Directory policies.

If you are not using Azure Active Directory, you can still layer Duo's authentication and access policies on top of Office 365 (or any cloud-based application) using the Security Assertion Markup Language (SAML) 2.0 standard. Duo's secure single sign-on solution can enforce role-based and device-based security policies before permitting access to Office 365 and other applications.



Protecting Windows Desktop

Many companies use Windows RDP to provide end users remote access to a number of business applications. Today, businesses are even deploying these desktop infrastructures in the public cloud for better scale and availability. Protecting access to local and remote Windows desktop sessions is critical to security. Duo can protect any Windows desktop environment, regardless of whether they are hosted on-premises or in the cloud.

Enforcing Trust on Windows Devices

Duo collects data about the status of each device upon access, and can enforce security policies based on the hygiene of those devices. For example, it can tell if the Windows version installed on the device complies with the security standards set by the company or if various Microsoft browsers like Internet Explorer and Edge are out-of-date and vulnerable to exploits.

It can even identify which Windows devices are managed by the company and which are personal, employee-owned machines. From there, Duo's policy engine allows you to create granular access policies to control which of these devices can access sensitive workloads and which cannot. Best of all, it can do this without deploying any agents on the endpoints, meaning it can easily cover both corporate-owned or personal devices.

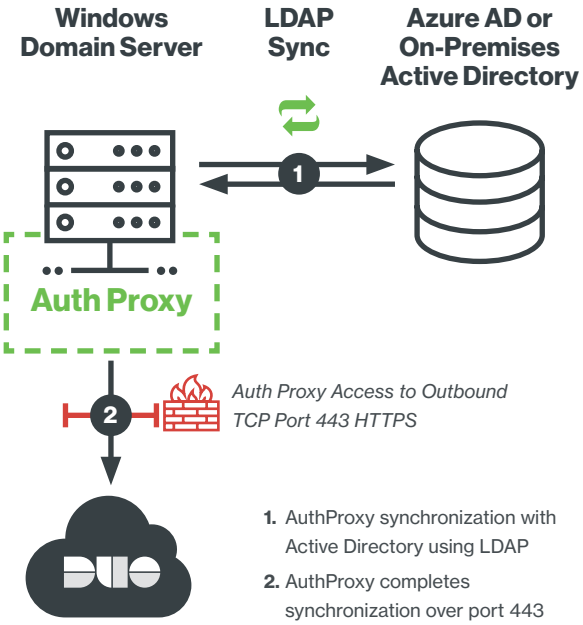
Leveraging Microsoft Directories

Many companies are deploying cloud-based Azure Active Directory (AD) to connect with popular cloud applications. Azure AD allows customers to extend their access security to Duo for a richer user experience and more granular policies. This can be configured directly within your Azure AD policies.

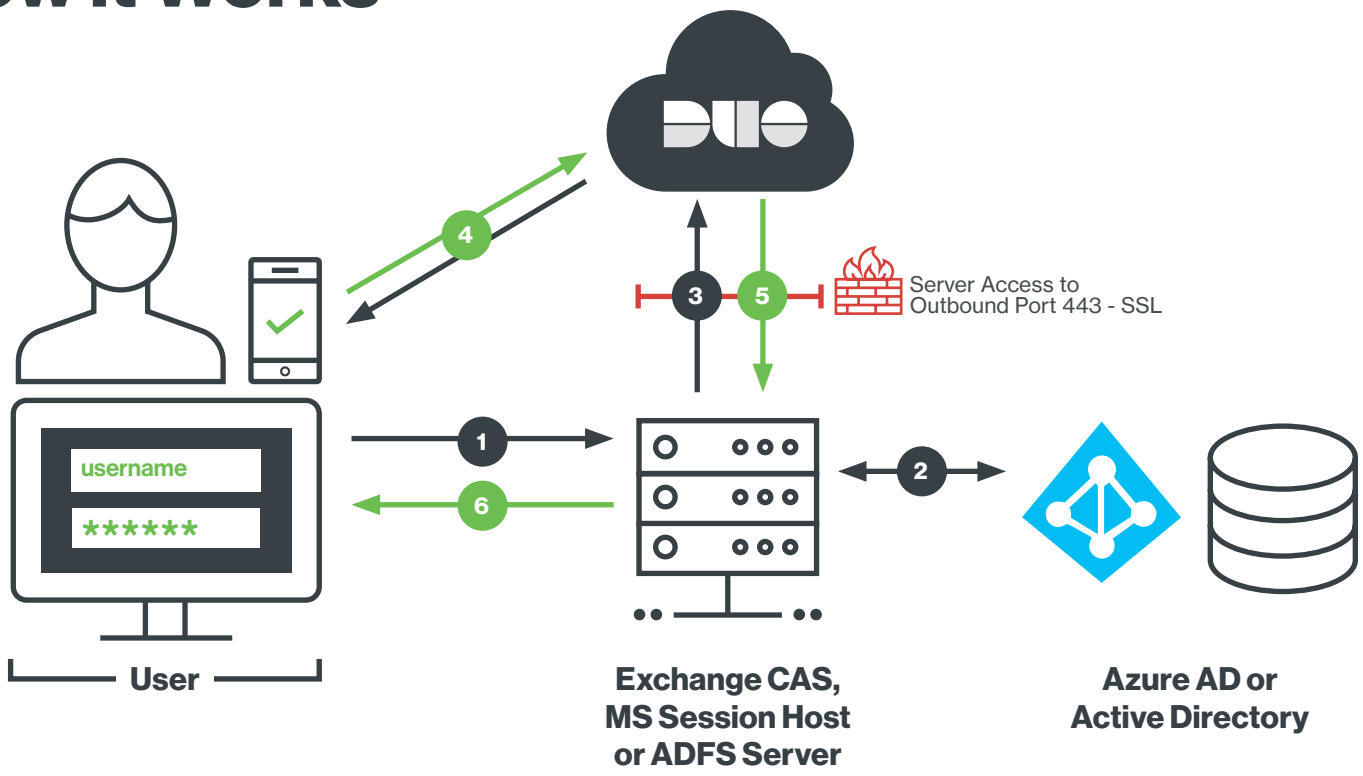
Organizations might also leverage Active Directory Federation Services (ADFS) to federate identities between multiple applications and AD instances. Duo can work with both on-premises and cloud-based AD and ADFS to enforce role-based policies for user access and authentication into any application.

By integrating Duo with ADFS, any browser-based application configured for federated logins against ADFS will be automatically protected with Duo.

Additionally, Duo offers Directory Sync capability with both on-premises and Azure Active Directory. In addition to the username, other directory attributes such as email, phone numbers, and group associations can also be automatically synced. You can configure Directory Sync against a single Active Directory server or a group of AD servers.



How it Works



With Outlook Web Access

1. User logs in to OWA with primary credentials.
2. Exchange CAS validates credentials with Active Directory.
3. Exchange CAServer connection established over TCP port 443.
4. Secondary authentication via Duo Push.
5. Duo sends approval back to Exchange CAS server.
6. User is granted access to OWA.

With RDP

1. User logs in to RDP session with primary credentials.
2. RDP session host validates credentials with Active Directory.
3. Sends credential validation to Duo cloud via Duo Windows Logon app.
4. Duo sends secondary authentication to user. User approves.
5. Duo sends approval back to the session host via Duo Windows Logon app.
6. User accesses RDP session.

With ADFS

1. User logs in to an ADFS connected application with primary credentials.
2. ADFS server validates credentials with Active Directory.
3. Sends credential validation to Duo via Duo ADFS app.
4. Duo sends secondary authentication to user. User approves.
5. Duo sends approval back to the ADFS server via Duo ADFS app.
6. User accesses the ADFS connected application.

The Trusted Access Company

Duo Security makes security painless, so you can focus on what's important. Our scalable, cloud-based **Trusted Access** platform addresses security threats before they become a problem, by verifying the identity of your users and the health of their devices before they connect to the applications you want them to access.

Thousands of organizations worldwide use Duo, including Facebook, Toyota, Panasonic and MIT. Duo is backed by Google Ventures, True Ventures, Radar Partners, Redpoint Ventures and Benchmark. We're located from coast to coast and across the sea.

866.760.4247 **sales@duo.com** **duo.com**