AGILITY
2016
SOLUTIONS FOR AN APPLICATION WORLD
Securing and Simplifying Office 365 Deployments with F5

Jay Kelley
Senior Product Marketing Manager
What Is Office 365?
What Is Office 365?
Why Is Office 365 Important?
Why Is Office 365 Important?

Here's more proof that companies are jumping on Microsoft Office 365 like crazy

Microsoft's Office 365 surpasses Google Apps in enterprise cloud-based adoption

Microsoft Office 365 most-used Web business app, report says

Okta Customer Research Finds Office 365 Most Used Cloud Service
Why Is Office 365 Important?

Investor Relations

Earnings Release FY16 Q4
Microsoft Cloud Strength Highlights Fourth Quarter Results
Commercial cloud annualized revenue run rate exceeds $12.1 billion

REDMOND, Wash. – July 19, 2016 – Microsoft Corp. today announced the following results for the quarter ended June 30, 2016:

Microsoft Office 365 most-used Web business app, report says

Okta Customer Research Finds Office 365 Most Used Cloud Service
Revenue in Productivity and Business Processes grew 5% (up 8% in constant currency) to $7.0 billion, with the following business highlights:

- Office commercial products and cloud services revenue grew 5% (up 9% in constant currency) driven by Office 365 commercial revenue growth of 54% (up 59% in constant currency)
- Office consumer products and cloud services revenue grew 19% (up 18% in constant currency) with Office 365 consumer subscribers increasing to 23.1 million
- Dynamics products and cloud services revenue grew 6% (up 7% in constant currency) with Dynamics CRM Online paid seats growing more than 2.5x year-over-year
Why Is Office 365 Important?

- Productivity and Business Processes revenue increased $308 million or 5%, primarily due to higher revenue from Office. Revenue included an unfavorable foreign currency impact of approximately 3%.
- Office Commercial revenue increased $249 million or 5%, driven by higher revenue from Office 365 commercial, mainly due to growth in subscribers, offset in part by lower volume licensing revenue, reflecting a continued shift to Office 365 commercial. Revenue included an unfavorable foreign currency impact of approximately 4%.

Revenue in Productivity and Business Processes grew 5% (up 8% in constant currency) to $7.0 billion, with the following business highlights:

- Office commercial products and cloud services revenue grew 5% (up 9% in constant currency) driven by Office 365 commercial revenue growth of 54% (up 59% in constant currency).
- Office consumer products and cloud services revenue grew 19% (up 18% in constant currency) with Office 365 consumer subscribers increasing to 23.1 million.
- Dynamics products and cloud services revenue grew 6% (up 7% in constant currency) with Dynamics CRM Online paid seats growing more than 2.5x year-over-year.
Further Evidence of Office 365’s Rapid Adoption

Source: SkyHigh Cloud Adoption Report Q4 2015
Further Evidence of Office 365’s Rapid Adoption

Source: SkyHigh Cloud Adoption Report Q4 2015
Further Evidence of Office 365’s Rapid Adoption
Benefits of Migrating to Office 365

- Increases user productivity
- Work anywhere, anytime
- Enhanced collaboration
- Product familiarity
But There Are Challenges to Migrating, Too

On-premises vs. cloud vs. hybrid

Overestimating product robustness

Identity and access management
Identity and Access Management
Challenges of Office 365

- Underestimating the need for federated Single Sign-On (SSO)
- Selecting the best, most appropriate SSO
- Security as an afterthought
Challenges of Sharing Identification Across Any Application, Anywhere, Anytime

- **Silos of identity**
- **Identity can be on-premises, with apps and data moving to the cloud**
- **Users experiencing “password fatigue”**
Three Identity Models for Office 365

Cloud Identity

User
Three Identity Models for Office 365

Cloud Identity

User → Salesforce → Office 365
Three Identity Models for Office 365

Synchronized Identity

Office 365

DirSync Tool

On-Premises Directory

User
Three Identity Models for Office 365

Synchronized Identity

Office 365

Sign-on

User

DirSync Tool

On-Premises Directory
Three Identity Models for Office 365

Federated Identity

Office 365

Synchronized Identity

User

On-Premises Directory

AD FS

DirSync Tool
Three Identity Models for Office 365

Federated Identity

- Office 365
- Synchronized Identity
- User
- Sign-on
- Authentication
- AD FS
- DirSync Tool
- On-Premises Directory
- Password hashes
- User accounts
- Authentication
Why Microsoft Active Directory Federation Service (AD FS) Is Not Always the Best Option

- Cannot replace IAM solutions
- Infrastructure costs increase TCO, depending on situation
- Need scaling/load-balancing
- Cannot integrate with full range of multi-factor authentication (MFA) solutions
- Cannot perform device posture checks before issuing assertion
Why Password Sync May Not Be the Best Option

- Have AD FS deployed
- Have on-premises smart card or MFA
- Require sign-in audit and/or immediate disable
- Policy preventing password hash synchronization to Azure Active Directory
- Use a third-party federated identity provider
- Custom hybrid apps and/or search required
- Requires single sign-on
- Use Forefront Identity Manager 2010 R2
- Web-accessible password reset
- Sign-in restrictions by location or time of day
F5 Access Policy Manager (APM)

Authentication, Authorization, and SSO from Any Device to All Apps, Anywhere, Anytime

- VDI/Virtual Apps
- Native VDI
- Secure Web Gateway
- Internet
- Web Malware
- Websites and Applications
- Web-Based Apps
- Web Access Management
- Remote Access and Application Access
- Enterprise Applications
- Mobile Apps
- Enterprise Mobility Gateway
- Identity Federation and SSO
- Virtual Edition
- Appliance
- Chassis

© 2016 F5 Networks
F5 Access Policy Manager (APM)

Authentication, Authorization, and SSO from Any Device to All Apps, Anywhere, Anytime

- VDI/Virtual Apps
- Native VDI
- Secure Web Gateway
- Internet
- Web Malware
- Websites and Applications
- Web-Based Apps
- Web Access Management
- Remote Access and Application Access
- Enterprise Applications
- Mobile Apps
- Enterprise Mobility Gateway
- Identity Federation and SSO
- Cloud, SaaS, VDI, Partner Apps

© 2016 F5 Networks
Identity Federation with Multi-Factor Authentication

XYZ Corporation

PUBLIC CLOUD
PRIVATE CLOUD

ACCESS POLICY ENFORCEMENT

MULTI-FACTOR AUTHENTICATION

Corporate Users

Directory Services

Corporate Applications

Office 365

© 2016 F5 Networks
F5 Has Been Working with Office 365
F5 Has Been Working with Office 365

- F5 has been working with Office 365 and federating users to Office 365 since BIG-IP v11.3
F5 Has Been Working with Office 365

• F5 has been working with Office 365 and federating users to Office 365 since BIG-IP v11.3
• F5 publishes an official Office 365 deployment guide and iApp
F5 Has Been Working with Office 365

• F5 has been working with Office 365 and federating users to Office 365 since BIG-IP v11.3


• Microsoft *officially supports* third-party SAML providers: “Third party SAML Providers are supported with Modern Auth Office 365 clients without having the need to validate them with the Works with Office 365 program” https://msdn.microsoft.com/enus/library/azure/dn641269.aspx
F5 Has Been Working with Office 365

- F5 has been working with Office 365 and federating users to Office 365 since BIG-IP v11.3
- Microsoft officially supports third-party SAML providers: “Third party SAML Providers are supported with Modern Auth Office 365 clients without having the need to validate them with the Works with Office 365 program” https://msdn.microsoft.com/enus/library/azure/dn641269.aspx
Visual Policy Editor (VPE)

Policies can be created in VPE so BIG-IP APM can redirect certain mailboxes to Office 365 while hosting others on premises.
Flexible, Context-Aware Authentication

Offers flexible context-aware authentication to Outlook clients
Flexible, Context-Aware Authentication
Flexible, Context-Aware Authentication
A Rich, Powerful Ecosystem of MFA Partners
F5 Webtop – How This Might Look to a User
F5 Webtop – How This Might Look to a User
F5 Webtop – How This Might Look to a User
F5 Webtop – How This Might Look to a User
Exchange Hybrid Federation Scenario

User Mailbox On-premises

Microsoft Azure

Office 365

On-Premises Infrastructure

login.contoso.com
mail.contoso.com

Active Directory
CAS Array

APM
Exchange Hybrid Federation Scenario

- Organizations that have deployed Office 365 but maintain user email boxes on-premises.
1. User connects to BIG-IP APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)

- Organizations that have deployed Office 365 but maintain user email boxes on-premises
Exchange Hybrid Federation Scenario

User Mailbox On-premises

1. User connects to BIG-IP APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. Exchange Service Provider (SP) Virtual sends user to Identity Provider (IdP) login.contoso.com with SAML AuthN request

• Organizations that have deployed Office 365 but maintain user email boxes on-premises
Exchange Hybrid Federation Scenario

1. User connects to BIG-IP APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. Exchange Service Provider (SP) Virtual sends user to Identity Provider (IdP) login.contoso.com with SAML AuthN request
3. User enters their credentials and is authenticated to login service

- Organizations that have deployed Office 365 but maintain user email boxes on-premises
1. User connects to BIG-IP APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)

2. Exchange Service Provider (SP) Virtual sends user to Identity Provider (IdP) login.contoso.com with SAML AuthN request

3. User enters their credentials and is authenticated to login service

4. Login responds with SAML Assertion that contains user’s username and password, which is sent to Outlook Web Access (OWA) SP

- Organizations that have deployed Office 365 but maintain user email boxes on-premises
Exchange Hybrid Federation Scenario

1. User connects to BIG-IP APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. Exchange Service Provider (SP) Virtual sends user to Identity Provider (IdP) login.contoso.com with SAML AuthN request
3. User enters their credentials and is authenticated to login service
4. Login responds with SAML Assertion that contains user’s username and password, which is sent to Outlook Web Access (OWA) SP
5. Exchange SP Policy checks if the user is on-premises and forwards to CAS

• Organizations that have deployed Office 365 but maintain user email boxes on-premises
Exchange Hybrid Federation Scenario

1. User connects to BIG-IP APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. Exchange Service Provider (SP) Virtual sends user to Identity Provider (IdP) login.contoso.com with SAML AuthN request
3. User enters their credentials and is authenticated to login service
4. Login responds with SAML Assertion that contains user’s username and password, which is sent to Outlook Web Access (OWA) SP
5. Exchange SP Policy checks if the user is on-premises and forwards to CAS

- Organizations that have deployed Office 365 but maintain user email boxes on-premises
- BIG-IP APM enables single sign-on (SSO) to Office 365 apps, while ensuring appropriate authentication to local/on-premises mailbox
- Simplifies the user experience via SSO to on-premises email and Office 365 apps
- Ensures that users and devices attempting to access Office 365 apps are authorized to do so
Exchange Hybrid Federation Scenario

User Mailbox Hosted in Office 365

- Microsoft Azure
- Office 365

On-Premises Infrastructure

- APM
- login.contoso.com
- maill.contoso.com

Active Directory

CAS Array
Exchange Hybrid Federation Scenario

User Mailbox Hosted in Office 365

- Organizations that have deployed Office 365, including user mailboxes
Exchange Hybrid Federation Scenario

1. User goes to https://mail.contoso.com

User Mailbox Hosted in Office 365

- Organizations that have deployed Office 365, including user mailboxes

 CAS Array

On-Premises Infrastructure

Microsoft Azure

Office 365

login.contoso.com
maill.contoso.com

Active Directory

APM
Exchange Hybrid Federation Scenario

1. User goes to https://mail.contoso.com
2. Exchange SP Virtual sends them to IdP login.contoso.com with SAML AuthN request

• Organizations that have deployed Office 365, including user mailboxes
Exchange Hybrid Federation Scenario

1. User goes to https://mail.contoso.com
2. Exchange SP Virtual sends them to IdP login.contoso.com with SAML AuthN request
3. User enters their credentials and authenticates to login service

- Organizations that have deployed Office 365, including user mailboxes
Exchange Hybrid Federation Scenario

1. User goes to https://mail.contoso.com
2. Exchange SP Virtual sends them to IdP login.contoso.com with SAML AuthN request
3. User enters their credentials and authenticates to login service
4. Login responds with SAML Assertion that contains username and password, it gets sent to https://mail.contoso.com

- Organizations that have deployed Office 365, including user mailboxes

User Mailbox Hosted in Office 365
Exchange Hybrid Federation Scenario

1. User goes to https://mail.contoso.com
2. Exchange SP Virtual sends them to IdP login.contoso.com with SAML AuthN request
3. User enters their credentials and authenticates to login service
4. Login responds with SAML Assertion that contains username and password, it gets sent to https://mail.contoso.com
5. Exchange SP Policy determines user is hosted in Office 365 and redirects them to https://outlook.com/owa/contoso.com

- Organizations that have deployed Office 365, including user mailboxes
Exchange Hybrid Federation Scenario

2. Exchange SP Virtual sends them to IdP login.contoso.com with SAML AuthN request.
3. User enters their credentials and authenticates to login service.
4. Login responds with SAML Assertion that contains username and password, it gets sent to https://mail.contoso.com.
5. Exchange SP Policy determines user is hosted in Office 365 and redirects them to https://outlook.com/owa/contoso.com.
6. Office 365 sends authentication request to login.contoso.com.

- Organizations that have deployed Office 365, including user mailboxes.
Exchange Hybrid Federation Scenario

1. User goes to https://mail.contoso.com
2. Exchange SP Virtual sends them to IdP login.contoso.com with SAML AuthN request
3. User enters their credentials and authenticates to login service
4. Login responds with SAML Assertion that contains username and password, it gets sent to https://mail.contoso.com
5. Exchange SP Policy determines user is hosted in Office 365 and redirects them to https://outlook.com/owa/contoso.com
6. Office 365 sends authentication request to login.contoso.com
7. Login.contoso.com IdP responds with SAML assertion (user has already authenticated to it in step 3) and user is signed on to OWA in the Office 365

• Organizations that have deployed Office 365, including user mailboxes
1. User goes to https://mail.contoso.com
2. Exchange SP Virtual sends them to IdP login.contoso.com with SAML AuthN request
3. User enters their credentials and authenticates to login service
4. Login responds with SAML Assertion that contains username and password, it gets sent to https://mail.contoso.com
5. Exchange SP Policy determines user is hosted in Office 365 and redirects them to https://outlook.com/owa/contoso.com
6. Office 365 sends authentication request to login.contoso.com
7. Login.contoso.com IdP responds with SAML assertion (user has already authenticated to it in step 3) and user is signed on to OWA in the Office 365

- Organizations that have deployed Office 365, including user mailboxes
- BIG-IP APM enables single sign-on (SSO) to Office 365 hosted mailboxes and apps, while alleviating the need to move user credentials to the cloud
- Eliminates the cost of moving user credentials to the cloud
- Mitigates the risk of user credentials being lost or stolen in a cloud breach
A Potential Security Risk

User Mailbox Hosted in Office 365

Microsoft Azure
Office 365

On-Premises Infrastructure

login.contoso.com
Active Directory
A Potential Security Risk

User Mailbox Hosted in Office 365

- Organizations that are moving or have migrated their email to Office 365, and are using Azure Active Directory (AD) for authentication
A Potential Security Risk

1. ActiveSync Client connects to https://outlook.office365.com and sends the user’s credentials via Basic Authentication

- Organizations that are moving or have migrated their email to Office 365, and are using Azure Active Directory (AD) for authentication
A Potential Security Risk

1. ActiveSync Client connects to https://outlook.office365.com and sends the user’s credentials via Basic Authentication
2. Exchange Online holds the request and sends it to Azure Active Directory security token service (STS)

- Organizations that are moving or have migrated their email to Office 365, and are using Azure Active Directory (AD) for authentication
A Potential Security Risk

1. ActiveSync Client connects to https://outlook.office365.com and sends the user’s credentials via Basic Authentication
2. Exchange Online holds the request and sends it to Azure Active Directory security token service (STS)
3. Azure Active Directory STS sends a SAML AuthN request to APM replaying the user’s credentials as Basic Authentication

• Organizations that are moving or have migrated their email to Office 365, and are using Azure Active Directory (AD) for authentication.
A Potential Security Risk

1. ActiveSync Client connects to https://outlook.office365.com and sends the user’s credentials via Basic Authentication
2. Exchange Online holds the request and sends it to Azure Active Directory security token service (STS)
3. Azure Active Directory STS sends a SAML AuthN request to APM replaying the user’s credentials as Basic Authentication

- Organizations that are moving or have migrated their email to Office 365, and are using Azure Active Directory (AD) for authentication

Azure Active Directory accesses and processes user credentials in **clear text**!!

© 2016 F5 Networks
A Potential Security Risk

1. ActiveSync Client connects to https://outlook.office365.com and sends the user’s credentials via Basic Authentication
2. Exchange Online holds the request and sends it to Azure Active Directory security token service (STS)
3. Azure Active Directory STS sends a SAML AuthN request to APM replaying the user’s credentials as Basic Authentication
4. APM authenticates the user against local Active Directory by extracting user’s Basic credentials.

Organizations that are moving or have migrated their email to Office 365, and are using Azure Active Directory (AD) for authentication

Azure Active Directory accesses and processes user credentials in clear text!!
A Potential Security Risk

1. ActiveSync Client connects to https://outlook.office365.com and sends the user’s credentials via Basic Authentication.

2. Exchange Online holds the request and sends it to Azure Active Directory security token service (STS).

3. Azure Active Directory STS sends a SAML AuthN request to APM replaying the user’s credentials as Basic Authentication.

4. APM authenticates the user against local Active Directory by extracting user’s Basic credentials.

5. Login.contoso.com IdP responds with SAML assertion to Azure STS.

• Organizations that are moving or have migrated their email to Office 365, and are using Azure Active Directory (AD) for authentication.

© 2016 F5 Networks

User Mailbox Hosted in Office 365

Azure Active Directory accesses and processes user credentials in clear text!!
A Potential Security Risk

1. ActiveSync Client connects to https://outlook.office365.com and sends the user’s credentials via Basic Authentication
2. Exchange Online holds the request and sends it to Azure Active Directory security token service (STS)
3. Azure Active Directory STS sends a SAML AuthN request to APM replaying the user’s credentials as Basic Authentication
4. APM authenticates the user against local Active Directory by extracting user’s Basic credentials.
5. Login.contoso.com IdP responds with SAML assertion to Azure STS
6. Azure STS then grants access to ActiveSync session to connect to the user’s mailbox in Office 365

- Organizations that are moving or have migrated their email to Office 365, and are using Azure Active Directory (AD) for authentication

On-Premises Infrastructure

User Mailbox Hosted in Office 365

Azure Active Directory accesses and processes user credentials in **clear text**!!
A Potential Security Risk

1. ActiveSync Client connects to https://outlook.office365.com and sends the user’s credentials via Basic Authentication
2. Exchange Online holds the request and sends it to Azure Active Directory security token service (STS)
3. Azure Active Directory STS sends a SAML AuthN request to APM replaying the user’s credentials as Basic Authentication
4. APM authenticates the user against local Active Directory by extracting user’s Basic credentials.
5. Login.contoso.com IdP responds with SAML assertion to Azure STS
6. Azure STS then grants access to ActiveSync session to connect to the user’s mailbox in Office 365

- Organizations that are moving or have migrated their email to Office 365, and are using Azure Active Directory (AD) for authentication
- Azure AD processes and sends user credentials in clear text, a major security concern
- If hackers were to tap into or intercept communications with plain text user credentials, or if Azure AD is hacked, customer network and data would be at grave risk
- User credentials would be processed “as is”, without being encrypted or protected in any manner
- For mobile devices, no support of endpoint checks by MDM/EMM is a concern
How F5 Addresses Potential Security Risk

User

Microsoft Azure

On-Premises Infrastructure

User Mailbox
Hosted in Office 365

User Mailbox
Hosted in Office 365

login.contoso.com
maill.contoso.com

Active Directory

© 2016 F5 Networks
How F5 Addresses Potential Security Risk

- BIG-IP APM serves as proxy for ActiveSync
How F5 Addresses Potential Security Risk

1. User connects to APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)

• BIG-IP APM serves as proxy for ActiveSync
How F5 Addresses Potential Security Risk

1. User connects to APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. APM encrypts user credentials and forwards request to Exchange Online in Office 365

- BIG-IP APM serves as proxy for ActiveSync

**User Mailbox Hosted in Office 365**

- On-Premises Infrastructure

**Microsoft Azure**

**Office 365**

**Active Directory**

**login.contoso.com**

**mail.contoso.com**
How F5 Addresses Potential Security Risk

User Mailbox Hosted in Office 365

- BIG-IP APM serves as proxy for ActiveSync

1. User connects to APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. APM encrypts user credentials and forwards request to Exchange Online in Office 365
3. Exchange Online holds the request and sends it to Azure AD security token service (STS)

© 2016 F5 Networks
How F5 Addresses Potential Security Risk

• BIG-IP APM serves as proxy for ActiveSync

1. User connects to APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. APM encrypts user credentials and forwards request to Exchange Online in Office 365
3. Exchange Online holds the request and sends it to Azure AD security token service (STS)
4. Azure AD STS sends SAML AuthN request to the IdP login.contoso.com (APM/ADFS/Ping, etc.)
How F5 Addresses Potential Security Risk

1. User connects to APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. APM encrypts user credentials and forwards request to Exchange Online in Office 365
3. Exchange Online holds the request and sends it to Azure AD security token service (STS)
4. Azure AD STS sends SAML AuthN request to the IdP login.contoso.com (APM/ADFS/Ping, etc.)
5. APM decrypts user’s credentials before processing them for authentication

- BIG-IP APM serves as proxy for ActiveSync
How F5 Addresses Potential Security Risk

1. User connects to APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. APM encrypts user credentials and forwards request to Exchange Online in Office 365
3. Exchange Online holds the request and sends it to Azure AD security token service (STS)
4. Azure AD STS sends SAML AuthN request to the IdP login.contoso.com (APM/ADFS/Ping, etc.)
5. APM decrypts user’s credentials before processing them for authentication
6. https://login.contoso.com IdP responds with SAML assertion to Azure STS
How F5 Addresses Potential Security Risk

1. User connects to APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. APM encrypts user credentials and forwards request to Exchange Online in Office 365
3. Exchange Online holds the request and sends it to Azure AD security token service (STS)
4. Azure AD STS sends SAML AuthN request to the IdP login.contoso.com (APM/ADFS/Ping, etc.)
5. APM decrypts user’s credentials before processing them for authentication
6. https://login.contoso.com IdP responds with SAML assertion to Azure STS
7. Azure STS then grants access to ActiveSync session to connect to the user’s mailbox in Office 365

- BIG-IP APM serves as proxy for ActiveSync
How F5 Addresses Potential Security Risk

1. User connects to APM as ActiveSync proxy (a.k.a., https://mail.contoso.com)
2. APM encrypts user credentials and forwards request to Exchange Online in Office 365
3. Exchange Online holds the request and sends it to Azure AD security token service (STS)
4. Azure AD STS sends SAML AuthN request to the IdP login.contoso.com (APM/ADFS/Ping, etc.)
5. APM decrypts user’s credentials before processing them for authentication
6. https://login.contoso.com IdP responds with SAML assertion to Azure STS
7. Azure STS then grants access to ActiveSync session to connect to the user’s mailbox in Office 365

- BIG-IP APM serves as proxy for ActiveSync
- APM encrypts the user credentials before forwarding them on to Office 365
- APM can integrate with existing MFA and IdP, such as AD FS, Ping Identity, and others
- Mitigates risk of hack, tap or interception of plain text user credentials while being communicated or stored
- Allows MDM/EMM based endpoint checks to be run
Addressing Mobile Federation Scenario

User Mailbox Hosted in Office 365

On-Premises Infrastructure

MDM/EMM Active Directory

login.contoso.com

Microsoft Azure

Office 365
Addressing Mobile Federation Scenario

- Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)

User Mailbox Hosted in Office 365

Microsoft Azure

Office 365

On-Premises Infrastructure

MDM/EMM Active Directory

MDM

Office 365

APM

login.contoso.com
Addressing Mobile Federation Scenario

1. Mobile user selects Office 365 apps from mobile device and is connected to BIG-IP APM via per-app VPN

- Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)

User Mailbox Hosted in Office 365
Addressing Mobile Federation Scenario

• Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)

1. Mobile user selects Office 365 apps from mobile device and is connected to BIG-IP APM via per-app VPN
2. APM checks user and device against MDM/EMM

User Mailbox Hosted in Office 365
Addressing Mobile Federation Scenario

1. Mobile user selects Office 365 apps from mobile device and is connected to BIG-IP APM via per-app VPN
2. APM checks user and device against MDM/EMM

• Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)

User Mailbox Hosted in Office 365

On-Premises Infrastructure

MDM/EMM device checks are crucial to ensure device and application security!
Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)

1. Mobile user selects Office 365 apps from mobile device and is connected to BIG-IP APM via per-app VPN
2. APM checks user and device against MDM/EMM
3. If user and device are okayed by MDM/EMM, APM, as ActiveSync proxy, encrypts user credentials and forwards request to Office 365; if not, user is denied Office 365 app access

MDM/EMM device checks are crucial to ensure device and application security!
Addressing Mobile Federation Scenario

1. Mobile user selects Office 365 apps from mobile device and is connected to BIG-IP APM via per-app VPN
2. APM checks user and device against MDM/EMM
3. If user and device are okayed by MDM/EMM, APM, as ActiveSync proxy, encrypts user credentials and forwards request to Office 365; if not, user is denied Office 365 app access
4. Office 365 sends SAML AuthN request to the IdP login.contoso.com

• Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)

MDM/EMM device checks are crucial to ensure device and application security!
Addressing Mobile Federation Scenario

1. Mobile user selects Office 365 apps from mobile device and is connected to BIG-IP APM via per-app VPN
2. APM checks user and device against MDM/EMM
3. If user and device are okayed by MDM/EMM, APM, as ActiveSync proxy, encrypts user credentials and forwards request to Office 365; if not, user is denied Office 365 app access
4. Office 365 sends SAML AuthN request to the IdP login.contoso.com
5. APM decrypts user’s credentials before processing them for authentication

• Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)
Addressing Mobile Federation Scenario

- Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)

1. Mobile user selects Office 365 apps from mobile device and is connected to BIG-IP APM via per-app VPN
2. APM checks user and device against MDM/EMM
3. If user and device are okayed by MDM/EMM, APM, as ActiveSync proxy, encrypts user credentials and forwards request to Office 365; if not, user is denied Office 365 app access
4. Office 365 sends SAML AuthN request to the IdP login.contoso.com
5. APM decrypts user’s credentials before processing them for authentication
6. APM responds with SAML assertion to Office 365

MDM/EMM device checks are crucial to ensure device and application security!
Addressing Mobile Federation Scenario

1. Mobile user selects Office 365 apps from mobile device and is connected to BIG-IP APM via per-app VPN
2. APM checks user and device against MDM/EMM
3. If user and device are okayed by MDM/EMM, APM, as ActiveSync proxy, encrypts user credentials and forwards request to Office 365; if not, user is denied Office 365 app access
4. Office 365 sends SAML AuthN request to the IdP login.contoso.com
5. APM decrypts user’s credentials before processing them for authentication
6. APM responds with SAML assertion to Office 365
7. Office 365 grants access to ActiveSync session to connect to the user’s mailbox in Office 365

- Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)

MDM/EMM device checks are crucial to ensure device and application security!
Addressing Mobile Federation Scenario

1. Mobile user selects Office 365 apps from mobile device and is connected to BIG-IP APM via per-app VPN
2. APM checks user and device against MDM/EMM
3. If user and device are okayed by MDM/EMM, APM, as ActiveSync proxy, encrypts user credentials and forwards request to Office 365; if not, user is denied Office 365 app access
4. Office 365 sends SAML AuthN request to the IdP login.contoso.com
5. APM decrypts user’s credentials before processing them for authentication
6. APM responds with SAML assertion to Office 365
7. Office 365 grants access to ActiveSync session to connect to the user’s mailbox in Office 365

• Organizations requiring secure identity federation for Office 365 apps from mobile devices that have deployed mobile device management (MDM)/enterprise mobility management (EMM)
• Enables APM per-app access, integrates with most leading, deployed MDM/EMM offerings
• Ensures secure identity federation to Office 365 apps from mobile devices
• Assures that users attempting to access Office 365 apps are authorized to do so, and devices adhere to security baseline

MDM/EMM device checks are crucial to ensure device and application security!
Modern Authentication (Federated Identities)

User → Word Online → Microsoft → login.microsoftonline.com → BIG-IP APM
Modern Authentication (Federated Identities)

User

Word Online

Open a file

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)
Modern Authentication (Federated Identities)

User

Word Online

Request doc (no token)

401: need token from login.microsoftonline.com

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

login.microsoftonline.com

Word Online

Microsoft

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com[/authURL] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authURL] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

(verify username/password)
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

302 with SAML Assertion for login.microsoftonline.com

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET  login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

302 with SAML Assertion for login.microsoftonline.com

POST SAML Assertion to login.microsoftonline.com

login.microsoftonline.com

BIG-IP APM

© 2016 F5 Networks
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

302 with SAML Assertion for login.microsoftonline.com

POST SAML Assertion to login.microsoftonline.com

200: (return access/refresh token)

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

302 with SAML Assertion for login.microsoftonline.com

POST SAML Assertion to login.microsoftonline.com

200: (return access/refresh token)

(cache refresh token)

login.microsoftonline.com

BIG-IP APM
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authURL] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

302 with SAML Assertion for login.microsoftonline.com

POST SAML Assertion to login.microsoftonline.com

200: (return access/refresh token)

(cache refresh token)

Request doc (access token)

login.microsoftonline.com

BIG-IP APM

© 2016 F5 Networks
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

302 with SAML Assertion for login.microsoftonline.com

POST SAML Assertion to login.microsoftonline.com

200: (return access/refresh token)

Request doc (access token)

200: return doc

login.microsoftonline.com

BIG-IP APM

© 2016 F5 Networks
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

302 with SAML Assertion for login.microsoftonline.com

POST SAML Assertion to login.microsoftonline.com

200: (return access/refresh token)

Request doc (access token)

200: return doc

login.microsoftonline.com

BIG-IP APM

© 2013 F5 Networks
Modern Authentication (Federated Identities)

User

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authURL] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter username/password)

302 with SAML Assertion for login.microsoftonline.com

POST SAML Assertion to login.microsoftonline.com

200: (return access/refresh token)

Request doc (access token)

200: return doc

login.microsoftonline.com

BIG-IP APM

© 2016 F5 Networks
Why BIG-IP APM for Office 365 Deployments?
Enhanced security, simplicity, and scalability

- Provides identity federation, SSO, and flexible context-based multi-factor authentication for Office 365
- Supports hybrid Microsoft Exchange deployments
- Industry-standard federation protocol support
- Most scalable solution available—5X–10X over competition

- Leverages F5’s existing SSL visibility to deliver visibility and control over data managed in Office 365
- Integrates with 18+ different MFA vendors
- Built-in MFA – One-time password (OTP) via email, certificate checks
- Support for comprehensive device posture checks for verification of managed vs. unmanaged devices, etc.

Office 365 policy using APM’s Visual Policy Editor (VPE)
The industry’s only access solution with a simple GUI for creating/modifying context-aware policies
Additional Resources

Exchange Online Identity Models and Authentication Demystified

Demo—Protecting Office 365 Access with Duo MFA and F5

Demo—Protecting Office 365 Access with Symantec VIP and F5

Demo—Protecting Office 365 Access with Gemalto and F5
Contact Information

Jay Kelley, Senior Product Marketing Manager
j.kelley@f5.com
Give Feedback – Get Points!

- Add class to your personal schedule.
- Survey will pop up in Mobile App.
- Answer the multiple choice.
- Submit your question to complete.
- Receive 5 points!