Partner Use Cases

Secure Mobile Access Using F5 BIG-IP and IBM MaaS360

February 2016
# Table of Contents

Introduction ........................................................................................................................................... 3

Technology Brief ................................................................................................................................. 3
  F5 BIG-IP Access Policy Manager .................................................................................................. 3
  IBM MaaS360 Enterprise Mobility Management ........................................................................... 4

Combined Solution ............................................................................................................................. 5
  BIG-IP APM Device Posture Check Feature .................................................................................. 5

Prerequisites ........................................................................................................................................ 6
  Infrastructure .................................................................................................................................... 6
  IBM MaaS360 ................................................................................................................................. 6
  F5 BIG-IP System ............................................................................................................................ 6

Lab Environment ................................................................................................................................ 7

Use Cases ........................................................................................................................................... 8
  Use Case 1: Full SSL VPN Based on Device Compliance ............................................................... 8
    BIG-IP Configuration .................................................................................................................... 8
    MaaS360 Configuration .................................................................................................................. 23
  Use Case 2: Per-Application VPN Based on Device Compliance .................................................. 29
    BIG-IP Configuration .................................................................................................................... 29
    MaaS360 Configuration .................................................................................................................. 34
  Use Case 3: On-Demand VPN Based on Device Compliance .......................................................... 40
    BIG-IP Configuration .................................................................................................................... 40
    MaaS360 Configuration .................................................................................................................. 43
  Use Case 4: Kerberos Single Sign-On Over Network Access Tunnel ........................................... 47
    BIG-IP Configuration .................................................................................................................... 47
    MaaS360 Configuration .................................................................................................................. 52
  Use Case 5: Microsoft Exchange Email Integration ........................................................................ 56
    MaaS360 ActiveSync Profile Configuration ................................................................................ 57
    BIG-IP APM Configuration .......................................................................................................... 57

Conclusion ............................................................................................................................................ 58

Learn More .......................................................................................................................................... 58
Introduction

The use of mobile devices and applications to transform business processes is increasing at an unprecedented rate. As more and more enterprises migrate towards highly mobile environments, it can be difficult to consistently provide secured access to corporate data and applications. To add to this complexity, employees who introduce “Bring Your Own Devices” (BYODs) into the corporate network to access work email and other company information raise additional security concerns about the state of such devices. In order to enable the desired freedom while balancing risk, productivity, and privacy, companies need to make sure that these devices meet corporate compliance standards and are able to grant access and control based on the device posture information.

F5® BIG-IP® Access Policy Manager® (APM) integration with IBM® MaaS360 addresses this exact need. This document will cover a few use cases in which BIG-IP APM is implemented as an enterprise mobile gateway to control mobile access to corporate resources using the MaaS360 solution. This document will discuss in detail the setup and configuration of BIG-IP APM to integrate with MaaS360 solution as tested in the F5 solutions lab.

Technology Brief

F5 BIG-IP Access Policy Manager

BIG-IP Access Policy Manager is a flexible, high-performance access and security solution that provides unified global access to your applications and corporate networks. By converging and consolidating remote access, LAN access, web access, and wireless connections within a single management interface and providing simple, easy-to-manage access policies, BIG-IP APM helps you free up valuable IT resources while you cost-effectively secure and scale access.

BIG-IP APM works with an optional client, BIG-IP® Edge Client®, to enable secure remote access to networks, clouds, and applications. BIG-IP Edge Client helps ensure continued user productivity whether the user is at home on a wireless network, using an air card in transit, giving a presentation over corporate wireless, in a café on guest wireless, or docked on a LAN connection. BIG-IP Edge Client for mobile devices provides full network access through BIG-IP APM. With network access, users can run enterprise applications on their mobile devices. Figure 1 shows the high level architecture of BIG-IP APM as secured access gateway.
IBM MaaS360 Enterprise Mobility Management

IBM MaaS360® Enterprise Mobility Management (EMM) provides complete visibility and control to support mobile devices in the enterprise. IBM MaaS360 works in conjunction with various other components that are hosted in your network, to deliver a complete device and application management solution. The MaaS360 Active Directory integration capability is an optional component that can be configured to provide device authentication and access group information.

MaaS360® Cloud Extender (CE) is a small program that runs as a service on a Microsoft Windows server in your network. The CE creates an outbound connection over HTTPS to the MaaS360 portal that is used for bi-directional communication. The MaaS360 CE for Active Directory (AD) integrates with your AD Server to provide the necessary interaction. Figure 2 below illustrates the major components of the IBM MaaS360 EMM solution that help ensure devices remain compliant based on defined policies.

This document only covers scenarios tested on MaaS360 cloud-based deployment.
**Combined Solution**

Prior to the BIG-IP v12.0 release, BIG-IP integration with MaaS360 had been mostly on the client side, which enabled provisioning of the BIG-IP Edge Client application using MaaS360 on mobile devices. This provisioned Edge Client application was then used to initiate VPN connections from mobile devices. With BIG-IP v12.0, additional server-side support has been added for BIG-IP APM to make VPN connections more intelligently based on important mobile device information from MaaS360.

**BIG-IP APM Device Posture Check Feature**

BIG-IP APM’s Device Posture Check (DPC) feature is introduced in BIG-IP v12.0. Using DPC, certain important information can be obtained about a mobile device from which SSL VPN connections are instantiated to BIG-IP APM through Application Program Interface (API) calls. This information includes device enrollment and compliance information in accordance with corporate standards.

Using the DPC, endpoint management system objects can be configured on BIG-IP to control access and usage of corporate data on mobile devices. In this case, the endpoint management system is IBM MaaS360. When a VPN connection is initiated from a mobile device, BIG-IP leverages these configurations to undertake necessary checks on the connecting mobile device. This entails a device information cache lookup or a request to the MaaS360 endpoint management system to grant access to the corporate network.

MaaS360 manages its enrolled device details, and provides these details to BIG-IP APM periodically or when a BIG-IP Edge Client application on the mobile device initiates a VPN connection.

For more detailed information on this feature, please refer to the [DPC technical documentation](#).
Prerequisites

**Infrastructure**

In order to deploy this solution (as tested in the F5 solutions lab), the following infrastructure pre-requisites are required:

- A DNS server
- An Active Directory server
- An NTP time server
- One globally routable IP address for BIG-IP virtual IP configuration
- iOS and Android mobile device(s) with network access
- Mobile device(s) with BIG-IP Edge Client application v2.0.5+ and MaaS360 client application v2.95.116 installed
- BIG-IP administrator login credentials
- Certificate Service setup

**IBM MaaS360**

- MaaS360 cloud account
Partner Use Cases
F5 APM-IBM MaaS360 Integration

- Obtained via MaaS360 free trial or from the IBM account team
  - Application ID, version, platform, and access key information from MaaS360 account team
  - MaaS360 CE setup for user authentication, certificate integration, and Exchange ActiveSync integration

**F5 BIG-IP System**
- BIG-IP v12.0 physical or virtual edition instance with networking configured (VLANs, self IPs, route)
- BIG-IP license for BIG-IP APM software module
  - This license should include enough concurrent user sessions as required per the use case and deployment

**Lab Environment**
Figure 4 shows the integrated solution setup in the F5 solutions lab:
Use Cases

The BIG-IP Edge Client application provides users with two main options (use cases) to establish a VPN tunnel connection. The first option is to explicitly start a tunnel connection with the BIG-IP Edge Client application. The second option is to implicitly connect through the on-demand functionality. On-Demand VPN itself can be implemented either as a per-application VPN or per-domain VPN.

The client-side provisioning options above have been thoroughly tested and are already widely used with MaaS360. The following use cases will discuss BIG-IP APM server-side implementation for each of these options to obtain crucial mobile device posture information (DPC) from MaaS360 and make more intelligent decisions when establishing VPN connections using the BIG-IP Edge Client application.

Use Case 1: Full SSL VPN Based on Device Compliance

This use case illustrates full SSL VPN connection from mobile devices for every request made from a managed mobile client that is compliant with MaaS360 policies. Full SSL VPN functionality has been successfully tested on both Android, as shown in this use case, and iOS platforms.

BIG-IP Configuration

This section will cover the steps required to configure BIG-IP APM through the web configuration utility.

Remote Access Wizard

The BIG-IP configuration utility wizard will assist you in creating a remote access configuration using BIG-IP APM. Log in to the BIG-IP system and select Wizards > Device Wizards from the left menu bar. Select Network Access Setup Wizard for Remote Access and click Next.

Enter a Policy Name and Caption. The default language, webtop, and client anti-virus checks are optional. Then click Next to continue.
Select the **Authentication Option**. Select an existing one or **Create New**. Select the **Authentication Server Type** from the list. In this example we choose an AD Authentication method. Then click **Next** to continue to configure authentication server details.

In the next screen (Figure 8), enter a **Domain Name**, and choose **Use Pool** connection to the Primary Domain Controller. Enter **IP Address**, **Hostname**, and add to the list of Domain Controllers. Provide **Admin Name** and **Password** for the AD Domain. Then click **Next** to continue.
BIG-IP will assign a lease pool - a pool of available IP addresses to remote clients for network access. The size of this pool needs to be large enough to provide enough address space for the total concurrent connections licensed by BIG-IP APM. In Figure 9, an address space of 20 IP addresses is defined. Enter an IP Version and a Start and End IP Address in a range. Select Add to move the address range to the Member List. Click Next to continue.
The client settings should be set according to the deployment scenario requirements. In Figure 10, we use split tunneling for traffic on 10.23.135.x LAN address space. Select **Use split tunneling for traffic** and provide both the **IP Address** and the **Mask**. Then click **Next** to continue.
Figure 10: Client Traffic Settings

Name Servers need to be specified. Enter a **Primary** and/or **Secondary Name Server** and the **Default Domain Suffix**.
Lastly, the virtual server IP address needs to be defined. A redirect virtual server will also be created. This will redirect client requests to the HTTPS virtual server. Enter an **IP Address** that is globally routable and resolvable by DNS. In this case, the IP address 206.124.129.95 resolves globally to F5MAASTEST.NET domain. Click **Next** to continue.

The wizard will display a list of all the configuration values entered. Review the list and click **Next** to continue. You may click **Previous** to correct any configuration mistakes.
### Figure 13: Access Wizard Configuration Review Details

<table>
<thead>
<tr>
<th>Wizard Type</th>
<th>Policy Name</th>
<th>Default Language</th>
<th>Enable AntiVirus Check in Access Policy</th>
<th>Full Webtop</th>
<th>Authentication Type</th>
<th>Domain Name</th>
<th>Admin Name</th>
<th>Admin Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Access Setup</td>
<td>F5_MaaS360_Policy</td>
<td>en</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Active Directory</td>
<td>f5maaas360.net</td>
<td>administrator</td>
<td>*********</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Access Details</th>
<th>Compression</th>
<th>Traffic Options</th>
<th>IPV4 LAN Address Space</th>
<th>Allow Local Subnet</th>
<th>Prohibit routing table changes during Network Access connection</th>
<th>DTLS</th>
<th>Assigned IPV4 Lease Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No Compression</td>
<td>Use split tunneling for traffic</td>
<td>10.123.35.0/24 255.255.255.0</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>F5_MaaS360_Policy_f0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Server Details</th>
<th>Virtual Server IP Address</th>
<th>Create Routed Virtual Server (HTTP in HTTPS)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>205.124.129.94</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
The Setup Summary is displayed.

![Setup Summary Table](image)

### Post-Wizard BIG-IP Configuration Steps

The wizard will address most of the configuration tasks necessary. The next sections (Figure 15–28) will address post-wizard configuration steps that you must complete.

### Endpoint Management Systems Configuration

MaaS360 specific configurations have to be made in the endpoint management systems configuration. Navigate to **Access Policy > Profiles > AAA Servers > Endpoint Management Systems** and select **Create**. Enter details as follows. Details obtained from the MaaS360 account team including access key, application ID, platform, and application version will be needed to complete this configuration.
Save the configurations. Now you will see it in the list of Endpoint Management Systems objects. Note that the **Status** shows *Synchronized* indicating that the DNS for the MaaS360 server was successfully resolved as per the settings in Figure 15, and is able to synchronize device information and status changes.

If Endpoint Management Systems object **Status** does not show *Synchronized*, check in the BIG-IP APM log file (/var/log/apm) from the BIG-IP command line interface for any errors and correct accordingly.
SSL Certificate and Key Setup

This solution requires an SSL certificate and key pair be imported to BIG-IP APM. For this implementation, Microsoft Active Directory Certificate Service (ADCS) has been used for CA setup and client certificate generation. F5 solution article SOL14499 describes another way to set up certificates on the BIG-IP system using OpenSSL. The certificate generation and configuration procedures are beyond the scope of this document, but it is important to note that the common name of the certificate must correspond to the globally resolvable DNS name of the virtual IP address.

It is important that you generate the required certificate and key pair before continuing to the next section.

SSL Client Profile

An SSL Client Profile must be bound to the HTTPS virtual server created in the previous section. Follow the configuration procedures to create an SSL Client Profile: Navigate to Local Traffic > Profiles > SSL > Client and select Create. Enter a Name. Scroll down to the Client Authentication section. Check the Custom boxes for Client Certificate and choose Request to request client certificate if it exists. Check the custom check boxes for Trusted Certificate Authorities and Advertised Certificate Authorities and select the certificate that was imported from the previous section.
Figure 17: Client SSL Profile Settings

Virtual Server Configuration

Some virtual server properties will be required to be set additionally. Edit the virtual server configurations for **F5_MaaS360_Policy_vs** and modify as follows:

Under the **Access Policy** section, select the previously created access policy for the **Access Profile** and **Connectivity Profile**.
Partner Use Cases
F5 APM-IBM MaaS360 Integration

<table>
<thead>
<tr>
<th>Access Policy</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Profile</td>
<td>F5_MaaS360_Policy</td>
</tr>
<tr>
<td>Connectivity Profile</td>
<td>F5_MaaS360_Policy_cp</td>
</tr>
<tr>
<td>Per-Request Policy</td>
<td>None</td>
</tr>
<tr>
<td>VDI Profile</td>
<td>None</td>
</tr>
<tr>
<td>Application Tunnels (Java &amp; Per-App VPN)</td>
<td>Enabled</td>
</tr>
<tr>
<td>OAM Support</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Figure 18: Access and Connectivity profile Setting in virtual Server**

For **VLANs and Tunnels**, select the **External_VLAN** from the Available list and click the << button to move it to the Selected column. This is a security feature that prevents VLAN misuse.

**Figure 19: External VLAN Selection in Virtual Server**

Set the virtual server to use the SSL client and server profiles created in the previous section. Select the **SSL Profile** from the Available list and click the << button to move it to the Selected column. Click the >> button on the default profile from the Selected SSL column to move it to the Available column.

**Figure 20: Client SSL Profile Setting**

**Access Policy Manager—Visual Policy Editor**

The BIG-IP APM Visual Policy Editor (VPE) is a subordinate user interface (UI) that resides within the BIG-IP APM web configuration utility to assist with building access policies. Depending on the deployment scenario, it may be necessary to alter the access policy. Configure the VPE per the following configuration procedures:

**Access Policy Flow**

Access the current access policy by navigating to **Access Policy > Access Profiles > Access Profiles List**. The list of access policies is displayed.
Click on the Edit hyperlink from the F5_MaaS360_Policy policy row. The VPE is displayed. The current policy should look as follows:

Each of the hyperlink items in blue underscored text can be modified to address the deployment requirements. Below are some important actions used in the access policy.

**Logon Page Action**

Click on the hyperlink labeled Logon Page. This will display the Logon page properties tab. The top portion of the page details the parameters that will be presented to the user.

The lower portion of the page contains the customization parameters available.
Modify these values to satisfy site specific deployment requirements. Select Cancel or Save to return to the VPE.

**AD Authentication Action**

Click on the hyperlink labeled AD Auth. This will display the Authentication page properties tab.
Modify these values to satisfy your specific deployment requirements. Select **Cancel** or **Save** to return to the VPE.

**Managed Endpoint Status Action**

Click on the hyperlink **Managed Endpoint Status**. This will display the properties tab.

Choose the endpoint management system that we created in earlier steps. Select **Cancel** or **Save** to return to the VPE. Select the **Close** button when finished.

**Resource Assign Action**

Click on the hyperlink labeled **Resource Assign**. This will display the resource properties tab.
Modify these values to satisfy site-specific deployment requirements. Select Cancel or Save to return to the VPE. Select the Close button when finished.

**Managed Endpoint Notification Action**

Click on the hyperlink labeled Managed Endpoint Notification. This will display the properties tab. Modify values to provide a meaningful name, specify the endpoint management system object, and a message to display.

It is recommended to take these access policy options into consideration when deploying VPN Profiles for MaaS360. Once the test client can properly authenticate and obtain privileges, MaaS360 services can be configured.

If the client is unable to authenticate, review the APM log files in the BIG-IP command line interface (CLI) at /var/log/apm and /var/log/ltm.

**MaaS360 Configuration**

This section covers the steps required for EMM configuration via the MaaS360 web administration console (herein referred to as the MaaS360 portal).

**MaaS360 Portal Access**

The MaaS360 portal is the management interface to configure MaaS360. Login to the portal. The links on the top provide more details about devices, users, and policies that can be configured. In this deployment we integrated MaaS360 CE with AD server—hence, the AD users are automatically populated in the MaaS360 portal.
Partner Use Cases
F5 APM-IBM MaaS360 Integration

![User Directory](image)

**Figure 29: AD Users in MaaS360 Portal**

From this screen, devices can be added to users by clicking the **Add Device** link and submitting a request.

![Add Device Screen](image)

**Figure 30: Add Device Screen for xuser user**

A one-time passcode is entered to complete the user’s MaaS360 enrollment. Once enrolled, the association is reflected in the portal.
The devices are assigned with default security policies based on their OS. New security policies can be created and published if additional customizations are necessary.

Open the applied policy (Default iOS Policy) from Security > Policies option in the portal and click the VPN tab. Set the VPN type to F5 SSL. This will allow MaaS360 to use BIG-IP Edge Client to instantiate VPN connections on the device.
Partner Use Cases
F5 APM-IBM MaaS360 Integration

Figure 33: Security Policy VPN Setting to Enable F5 Integration

Full SSL VPN Based on Device Compliance Check Verification

It should now be possible to test the BIG-IP APM access policy from the mobile BIG-IP Edge Client application. This tests the integration of BIG-IP APM with respective authentication servers. In this deployment, an Android Samsung Galaxy tablet device is used.

Open the mobile device's BIG-IP Edge client application from the mobile device and test that the BIG-IP APM login prompt is properly displayed. Enter the FQDN or IP address of the BIG-IP APM protected virtual server. This implementation will use the FQDN (f5maastest.net) corresponding to the virtual IP (206.124.129.94) in the BIG-IP Edge Client configurations. The Secure Logon page should be displayed. Enter a valid username and password pair and click **Login** to continue.
After verifying login credentials with AD services, the connection is established and a success notification is received on the device.

Now that the VPN is successfully established, secured corporate applications can be accessed from the mobile device. Figure 36 shows a secured Microsoft SharePoint application called Team Talk, which can be successfully accessed after connecting to the VPN.
Partner Use Cases
F5 APM-IBM MaaS360 Integration

Figure 36: MaaS360 Success Notification and Corporate SharePoint application Access Details
Use Case 2: Per-Application VPN Based on Device Compliance

Per-app VPN gives IT granular control over corporate network access. It ensures that the managed application traffic only flows through a VPN tunnel, and that any other application data does not use the VPN. Connections initiated for Per-app VPN do not allow user intervention. For example, if a password is required for authentication, but is not supplied in the configuration, the connection fails.

Per-app VPN configuration with MaaS360 is supported on both iOS 7+ and Android platforms. Applications that can be managed by MaaS360 can now be configured to automatically instantiate VPN connection when they are started.

The following section provides certificate-based configuration details for an iOS implementation using an iOS 8 device. Certificate-based authentication may be the most common way of implementing Per-app VPN, however user credential-based authentication is also supported as long as credentials are cached to avoid any user intervention.

BIG-IP Configuration

Core Component Setup

The BIG-IP configurations for this use case are an extension of the configurations we created for Use Case 1. The additional configurations below are required to set up per-app VPN.

Access Policy

Create a new access policy for per-app VPN by navigating to Access Policy > Access Profiles and select Create. Enter a Name and choose the Profile Type as All. Click Finished.

![Figure 37: Access policy creation details](image)

Navigate to Access Policy > Access Profiles > Access Profiles List. The list of access policies is displayed. Click on the Edit hyperlink for the access policy profile that we created above.

![Figure 38: Access policy list](image)
**Access Policy Manager—Visual Policy Editor**

Configure the VPE per the following configuration procedures to create a profile that inspects the client certificate and establishes a successful VPN after validating the device and application posture information from MaaS360.

![Visual Policy Editor Screen for Per Application VPN Policy](image)

**Client Cert Inspection Action**

This action is required to authenticate client certificate from where the application is launched to access VPN. No additional configurations are required for this action.

![Client Cert Inspection Action Details](image)

**Advanced Resource Assign Action**

This action assigns BIG-IP resources such as network, pool, and webtop to the client establishing the connection.

![Advanced Resource Assign Action Details](image)

The rest of the actions and policy flow are similar to what we created for the previous use case. After all the items are added, click the **Apply Access Policy** link on the top left of the screen to apply the changes.
Client SSL Profile

In the client SSL profile under Local Traffic. Profiles > SSL > Client, make sure the following configurations are set:

![Client SSL Profile Certificate Details](image)

*Figure 42: Client SSL Profile Certificate Details*
In the **Client Authentication** section, set the **Client Certificate** to **request** to check for the client certificate if presented at the time of connection. Provide the root certificate of the certification authority in the **Trusted** and **Advertised Certification Authorities** settings.

![Client SSL Profile CA Configuration Details](image)

The next step is to assign this profile to the virtual server.

**Virtual Server Advanced Configuration**

From the **Local Traffic > Virtual Servers > Virtual Server List**, open the virtual server that was previously created and modify as follows:
Specify the client SSL profile as described above and make sure the **Source Address Translation** is set to **Auto Map**.

In the Access Policy section of the virtual server settings, choose the following:
Click **Update** to save the above changes.

**MaaS360 Configuration**

**Certificate Integration**

For implementing Per-app VPN using certificate-based authentication, configuration of MaaS360 CE for certificate integration is a necessary step. In order to start with these configurations, make sure to:

- Use the same BIG-IP certification authority that generates certificates for mobile devices.
- Have NDES server set up to push client certificates to the managed mobile devices when a user accesses applications through the device.

For detailed configuration steps on MaaS360 CE, please refer to the [CE Certificate Authority Integration](#) documentation. This example implementation uses AD certificate service and NDES server set up on Microsoft Windows servers.

**Security Policy**

After the CE configurations are made and successfully tested, login to the MaaS360 portal and choose **SECURITY > Policies** option on the top menu. A list of policies is displayed.
Click **View** option on the policy that is assigned to your iOS device and choose the **Edit** option and **VPN** tab on the left menu to add VPN profile as illustrated in the below figure.

In this VPN configuration screen, provide the VPN host server FQDN that corresponds to the BIG-IP virtual server FQDN. Set the **User Authentication Type** as **Certificate** for certificate validation. For **Identity Certificate**, provide the certificate template name created in CE during certificate integration configuration. Check the “Include Device Details” option to pass additional device information to the VPN.
In the **Apps to use this VPN** region, specify the application name that you want to use to initiate a VPN connection. In this example, Dolphin Browser application for iOS will be used.

![Image of Dolphin Browser Application Configuration for Per-app VPN](image)

**Figure 49: Dolphin Browser Application Configuration for Per-app VPN**

Confirm and publish changes to the profile. This updated profile will then be applied to the iOS device it is linked to.

**Application Configuration**

Navigate to **APPS > Catalog** in the MaaS360 portal menu to add the Dolphin Browser application to the catalog and push it to the managed iOS device.

Click the **Add (iTunes AppStore App)** button from the dropdown menu on the top right of the screen and specify the same application used in the profile configuration.

![Image of Adding Dolphin Browser in Application Catalog](image)

**Figure 50: Adding Dolphin Browser in Application Catalog**

Save changes and the list of applications is updated with this newly added application.

![Image of App Catalog](image)

**Figure 51: Distributing Dolphin Browser Application**

Click the **Distribute** link for this application and specify the iOS device name you want to push this application and the install type.
Partner Use Cases
F5 APM-IBM MaaS360 Integration

Figure 52: Application Distribution Details

Shortly after, a request to install this application will appear on the device. Click install and provide required iTunes credentials. Once the application is installed, the application icon on the iPhone screen is displayed.

Figure 53: iPhone screen with Dolphin Browser Application Installed

Per-App VPN Verification

The VPN profile that was created in the MaaS360 policy appears on the iPhone device (F5_iOSVPN). Open the iPhone VPN settings to make sure there is no active VPN connection at this point.

Figure 54: BIG-IP Edge Client on iPhone with no active VPN connections
Open the Dolphin Browser on the iPhone to test Per-app VPN connectivity. Notice that the VPN connection does not yet appear on the top bar yet.

Figure 55: Dolphin Browser Application on iPhone

At this point, a VPN connection is instantiated by MaaS360 as configured in the MaaS360 iOS profile running on this iPhone. After successful connection establishment, a VPN icon is seen on the notification bar of the iPhone screen after a few seconds.

Figure 56: Successful VPN connection from the Dolphin browser application

With successful VPN connection, applications hosted in the internal corporate network can be accessed. In this implementation, an internal SharePoint application called Team Talk will be browsed from the Dolphin application.
A VPN connection is successfully established from Dolphin Browser application, thus demonstrating the working of per-application VPN.
Use Case 3: On-Demand VPN Based on Device Compliance

With On-Demand VPN, the operating system itself will determine when to trigger a VPN connection based on admin or user-defined policies through the MaaS360 portal. On-demand connections are triggered and initiated without any user intervention. The section below demonstrates configurations on iOS platform.

BIG-IP Configuration

Core Component Setup

BIG-IP configurations for this use case are an extension of the configurations we created for Use Case 1 or Use Case 2. Below are additional configurations that are required to set up on-demand VPN.

Access Policy

Create a new access policy for on-demand VPN by navigating to Access Policy > Access Profiles and select Create. Enter a Name, choose the Profile Type as All, and set English (en) in Accepted Languages in Language Settings. Click Finished.

![Image](image1.png)

Figure 58: On-Demand Access Profile Details

Navigate to Access Policy > Access Profiles > Access Profiles List. The list of access policies is displayed. Click on the Edit hyperlink for the access policy profile that we created above.

![Image](image2.png)

Figure 59: Access profile list details
Access Policy Manager—Visual Policy Editor

Configure the VPE per the following configuration procedures to create a profile that inspects the client certificate and establishes a successful VPN after validating the device and application posture information from MaaS360.

On-Demand Certificate Authentication Action

This action is used to authenticate a user by validating the client certificate against a server certificate. This action renegotiates the SSL connection to complete this validation.

Virtual Server Advanced Configuration

From the Local Traffic > Virtual Servers > Virtual Server List, edit the virtual server that was previously created and make the following modifications:
In the Access Policy section of the virtual server settings, choose the on-demand access policy that we created in earlier steps.

![Virtual server access policy configuration](image)

**Figure 63:** Virtual server access policy configuration

Make sure the Client SSL Profile and Source Address Translation are set as follows:

![Virtual server configuration details](image)

**Figure 64:** Virtual server configuration details

Click **Update** to save the settings.
MaaS360 Configuration

Certificate Integration

On-Demand VPN configuration also requires MaaS360 CE to be configured for certificate integration. Please refer to the Certificate Integration section of Use Case 2 in this document for more details.

Client certificate selection, delivery, and provisioning on mobile devices is completely taken care of by MaaS360 through the VPN settings in the MaaS360 security profile (refer to settings in figure below). Edge Client will then use that certificate on mobile device for certificate exchange accordingly when an implicit SSL connection is initiated.

![Figure 65: MaaS360 VPN setting for Certificates](image)

Security Policy

After the CE configurations are made and successfully tested, login to the MaaS360 portal and choose SECURITY > Policies option on the top menu. A list of policies is displayed.

![Figure 66: MaaS360 Security Policy list](image)

Click View option on the policy that is assigned to your iOS device. In this case, View the same security policy created for use case 2, click Edit and navigate to VPN tab on the left menu:
Scroll down in the policy to go to **Safari Domains to use this VPN** and provide application domain name to instantiate VPN connection when the same domain is browsed in Safari browser of iOS device.

Confirm and publish changes to the profile. This updated profile will then be applied to the iOS device it is linked to.
On-Demand VPN Verification

The mobile device screens in the following illustration are captured on iPhone 5 with iOS 9. Navigate to iPhone Settings > VPN to verify that there is no existing VPN connection.

Now open the Safari Web browser application on the device, and browse the application URL that was specified in the MaaS360 security policy earlier. Per the policy setting, a VPN connection is initiated and a notification is received on the iPhone about successful VPN establishment.

A VPN connection icon is displayed in the top notification bar. Soon after that, the internal corporate application login page is displayed, which authenticates the user and takes to the SharePoint application homepage.
On-demand VPN connection is successfully established by accessing the specified application in Safari web browser.
Use Case 4: Kerberos Single Sign-On Over Network Access Tunnel

Single Sign-On is an important feature that is part of BIG-IP APM’s rich feature set. By leveraging SSO technology, BIG-IP APM caches user credentials and reuses the cached identity to seamlessly log the user into the secured web applications, thus providing the user with a single sign on experience. This feature is even more useful for mobile users helping them to avoid typing the same details multiple times on smaller screens.

This use case is an extension of Use Case 2 and Use Case 3 to showcase BIG-IP APM’s SSO feature that can be leveraged to gain transparent access to corporate resources from mobile devices.

MaaS360 supports two types of authentication mechanisms: user credential-based authentication (username and password based) and certificate-based authentication. This use case will focus on Kerberos SSO implementation for certificate-based authentication.

![Diagram](image)

**Figure 72: Kerberos SSO Certificate-Based Authentication in BIG-IP APM**

**BIG-IP Configuration**

**Main Steps**

1. Validate AD
2. Set up Delegation User Account
3. Configure Kerberos SSO in APM
4. Configure Access Policy
5. Create Virtual Server for SSO

**Step 1—Validate AD**

Make sure all the involved AD domains are at Windows Server 2003 function level or higher.

**Step 2—Set up Delegation User Account in AD**

A delegation account is required to support Kerberos SSO. Create a delegation account in AD. Note that for every server realm, you must create a delegation account in that realm.

Open the AD Users and Computers administrative tool from Server Manager and create a new user account. The user account should be dedicated for delegation and the **Password never expires** setting enabled.

![Delegation Account Details](image)

Figure 73: Delegation Account Details

Run the `setspn` command-line tool for the user account from an elevated command prompt—where `apm` is the name of the user account and `f5maastest.net` is the Windows domain in which you create the user account.

```
setspn -S HOST/apm f5maastest\apm
```

The result for the delegation account can be verified by using the `setspn` command with the `-L` option.
setspn -L f5maastest\apm

Registered ServicePrincipalNames for
CN=apm,CN=Users,DC=F5MAASTEST,DC=NET: host/apm

Also, make sure the forward and reverse DNS is appropriately configured in DNS manager for server IP to resolve to hostname.

![Figure 74: Forward and Reverse Lookup Zone Configurations](image)

**Step 3—Configure Kerberos SSO in APM**

After making sure that the delegation user account is created and registered, create a Kerberos SSO configuration as follows:

1. On the Main tab, click **Access Policy > SSO Configurations > Kerberos**. The SSO Configurations screen opens for Kerberos type.

2. Click **Create**. The New SSO Configuration screen opens.

3. In the Name field, type a name for the SSO configuration.

4. In the Credentials Source area, specify the credentials that you want cached for Single Sign-On. Make sure the variable name provided for the Username Source has the correct username value populated from the certificate. This information can be obtained using **sessiondump--allkeys** admin command on the BIG-IP command line when the session is active.

5. In the Kerberos Realm field, type the name of the realm in uppercase—**F5MAASTEST.NET**.

6. In the Account Name field, type the name of the AD account configured for delegation.

7. In the Account Password and Confirm Account Password fields, type the delegation account password.
8. Click **Finished**.

![Figure 75: Kerberos SSO Object Configuration](image)

Also make sure the correct DNS address space is listed in the Network access configurations.

![Figure 76: Network Access Configuration for Network Settings](image)

**Step 4—Configure Access Policy**
A second access policy is required for this setup to associate SSO configurations. Go to Main tab > Access Policy >

Access Profiles and create a new access profile with the following settings:

![SSO Access Profile Configuration](image)

Figure 77: SSO Access Profile Configuration

In the SSO/Auth Domains tab, specify the SSO object created in the earlier steps.

![Access Profile SSO Setting](image)

Figure 78: Access Profile SSO Setting

For the access policy, no changes are required since it just acts as a dummy policy to inspect incoming traffic.

![Access Policy Details](image)

Figure 79: Access Policy Details

Please note that the original access policy configurations made for on-demand or per-app VPN remain unchanged.

**Step 5—Create Virtual Server for SSO**

In case of VPN, since the traffic leaves the VPN tunnel toward the destination before APM can inspect the traffic, configuration of another virtual server (layered virtual server) is required to capture some of this traffic and perform SSO. This second layered virtual server will use the SharePoint application server IP address as its virtual IP and be associated with the above created access profile (in step 4).
In order to instantiate VPN and apply SSO, the domain name of the SharePoint application will specified as one of the allowed Safari domains on MaaS360 portal. In this case, the IP address 10.23.135.11 corresponds to the hostname sharepoint1.5maastest.net.
Save and publish the policy to the devices.

**Verification**

To verify the working of certificate-based Kerberos SSO, an iPhone 5 with iOS 9 will be used. This iPhone is already enrolled with MaaS360 and is compliant with the policy published above. Open Safari browser on the iPhone. There is no active VPN connection at this point.
Browse to the SharePoint application containing “f5maastest.net” in the URL from Safari browser. A VPN connection will be instantiated and a success notification from MaaS360 will be displayed.

Immediately, the SharePoint application screen is displayed without prompting for any user credentials.
This concludes the verification of Kerberos SSO for SharePoint application over the network access tunnel.

The next use case is not based on device compliance, and is included in this document to showcase the value of using BIG-IP APM as ActiveSync Email Proxy with the MaaS360 mobile solution.
Use Case 5: Microsoft Exchange Email Integration

One of the most commonly used enterprise mobile applications is the email application. Mobile email access from mobile devices helps increase employee productivity, but can pose a serious security threat when accounting for corporate data leakages. Microsoft Exchange is one of the most popular choices for corporate emails, this use case will focus on Exchange integration.

BIG-IP APM provides secure remote email access. It supports the synchronization of email, calendar, and contacts with Microsoft Exchange on mobile devices that use the Microsoft ActiveSync protocol, such as the Apple iPhone. By eliminating the need for an extra tier of authentication gateways to accept Microsoft Outlook Web Access (OWA), ActiveSync, and Outlook Anywhere connections, BIG-IP APM helps you consolidate infrastructure and maintain user productivity.

MaaS360 integrates with ActiveSync infrastructure to simplify email administration and improve security and management. Using the MaaS360 web portal, appropriate email security policies (ActiveSync profiles) can be created and distributed to the managed mobile devices. These security policies help the native mobile email clients with the following:

- Identify the correct email server to connect (through certificates)
- Define who can access the emails (mobile user, third party applications, etc.)
- Define how to transfer data (handle attachments, email formats, etc.)

Below is the high level diagram for Exchange ActiveSync integration.
Detailed configurations for this set up will not be discussed in this document; please refer to the links below for detailed instructions surrounding this integration setup.

**MaaS360 ActiveSync Profile Configuration**

Steps to configure ActiveSync Profile using MaaS360

**BIG-IP APM Configuration**

Steps to configure BIG-IP APM as proxy for Microsoft Exchange ActiveSync
Conclusion

Allowing mobile access to secured corporate applications bring many security concerns to enterprises. A compromised mobile device, such as one that has been jail broken or rooted, can create disruptions such as lost productivity, missed opportunities, and damage to brand reputation.

When integrated with IBM MaaS360, F5 BIG-IP APM enables the best of both worlds to provide secure enterprise application access via managed and complaint mobile devices.

Learn More

You can explore this topic further with these resources:

BIG-IP APM Data Sheet
BIG-IP APM Support Documentation
BIG-IP APM Client Compatibility Matrix
BIG-IP APM SSO Configuration Guide
MaaS360 Documentation
MaaS360 Cloud Extender (CE) Setup
MaaS360 CE Certificate Integration Guide
Microsoft Active Directory (AD) Certificate Services Setup

Feedback on this document? Email mailto:appsteam@f5.com.

Ready to talk to F5? Email info@f5.com or call 206-272-5555.