MaaS360®
by Fiberlink

MaaS360 Cloud Extender Architecture

Fiberlink Communications Corporation

1787 Sentry Parkway West

Blue Bell, PA 19422

August 2013

029

Table of Contents

Introduction

The MaaS360 Platform is a multi-tenant, cloud-based platform for managing and securing laptops, smartphones and tablets, and the data that resides on them. Customers using MaaS360 reap the benefits of cloud technology that offers ease of deployment and low cost. To provide integration with important systems within the customer environment Fiberlink offers the MaaS360 Cloud Extender.

The patented MaaS360 Cloud Extender technology uses a lightweight agent. It can run with minimal resources; easily traverse customer proxy environments; and provide secure messaging and data transfer between the MaaS360 Platform and customer systems such as corporate email, corporate directories and application and content servers.

This document is intended to provide a high-level technology and architecture summary to help you gain confidence in the overall approach and to help plan and implement the MaaS360 solution. It should be referenced along with the MaaS360 quick start guides and the *MaaS360 Cloud Extender Installation Guide*. A list of these documents can be found in Appendix A.

Cloud Extender Overview and Architecture

The Cloud Extender is required for the following:

- **ActiveSync Auto-discovery, Quarantining and Blocking for MS Exchange 2007/2010/2013**—The MaaS360 Cloud Extender facilitates interaction with the ActiveSync Server and Active Directory. This allows MaaS360 to acquire information on ActiveSync-connected devices, upload device information to the MaaS360 Cloud, carry out actions sent from MaaS360 and apply ActiveSync device policies.
- **ActiveSync Auto-discovery for Lotus Traveler**—The MaaS360 Cloud Extender facilitates interaction with information acquired from Lotus Traveler about ActiveSync-connected devices, uploads device information to the MaaS360 Cloud and facilitates carrying out actions sent from MaaS360.
- **Corporate Directory Authentication**—The MaaS360 Cloud Extender facilitates interaction with Active Directory and LDAP to provide user validation as part of the self-service device enrollment and when authentication is required by policy for application and content access.
- **Corporate Directory User Views and Group Assignments**—The MaaS360 Cloud Extender leverages the corporate directory groups to allow for the assignment and distribution of policies, apps and docs. These groups are imported by the MaaS360 Administrator and can also be used to control administrator access.
- **Certificate Authority**—The MaaS360 Cloud Extender facilitates the automatic provisioning and distribution of digital certificates for wireless, VPN and email profiles to managed mobile devices using your existing Microsoft Certificate Authority or Symantec-hosted CA.
- **BlackBerry Enterprise Server (BES)**—The MaaS360 Cloud Extender uses the BES 5.0 Administrator APIs to provide complete visibility and control of BlackBerry devices.
- **Mobile Enterprise Gateway**—The Cloud Extender provides gateway and relay functionality, giving secure mobile application access to behind-the-firewall information and resources. This provides a more efficient and targeted approach than traditional VPNs.

The MaaS360 Cloud Extender is a small Windows executable (approx. 12MB) that is typically installed behind the customer firewall with network access to the appropriate internal systems. The MaaS360 Cloud Extender makes an outbound connection to the MaaS360 Cloud over port 443 (SSL AES256 encryption) and uses an XMPP style protocol to maintain the connection with the MaaS360 Cloud. The Cloud Extender is proxy-aware and can automatically configure proxy settings.

Once the connection is made, it is used to facilitate two-way communication between the MaaS360 Cloud and the Cloud Extender customer instance required for the integration functions.

The MaaS360 Cloud Extender is modular, and only the modules to support purchased features are installed. If a new feature is enabled, the related module and the associated configuration elements are automatically sent to the customer's Cloud Extender instance. All updates are automatic. The Cloud Extender's modular architecture provides mechanisms for module versioning and the limited release of modules to support pre-production testing.

MaaS360 Push Notification Service

Leveraging the outbound connection from the customer premises to MaaS360 facilitated by the Cloud Extender, MaaS360 administrators can send commands to the appropriate systems to achieve a specific result.

For example, when the administrator issues a Block command for a specific device from the MaaS360 Portal (or an automated rule needs to block a device), this command is sent the appropriate customer Cloud Extender instance. This instance will execute the command using APIs available on the email server. The result of the command is sent back to the MaaS360 Cloud to close the loop.

Data Collection and Upload

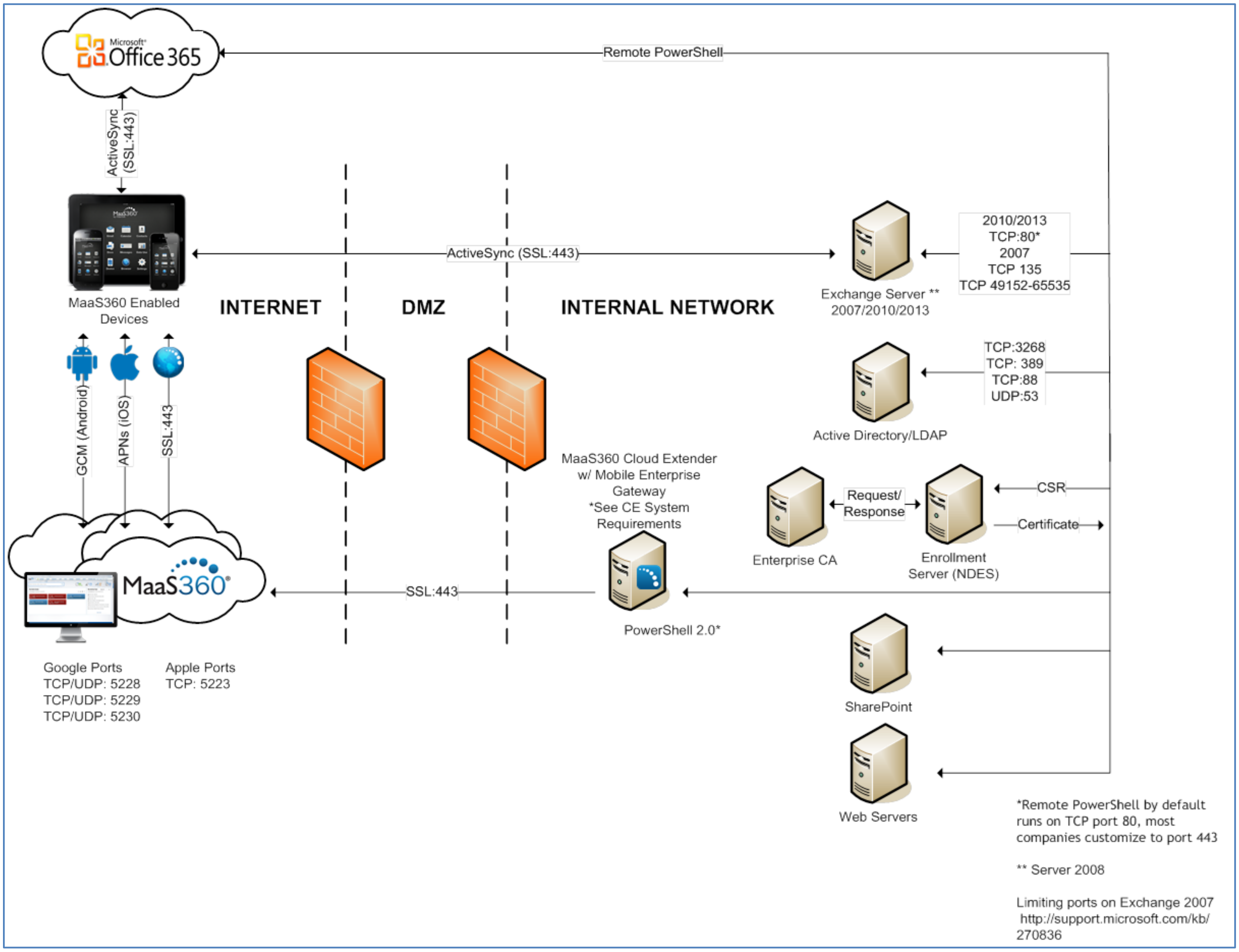
The Cloud Extender periodically queries for device and corporate directory information from customer systems, and uploads it to the MaaS360 Cloud for reporting and management functions.

Secure Gateway

The two-way communication channel provided between the MaaS360 Cloud and the customer's Cloud Extender is leveraged for secure access to internal web application servers and file repositories such as SharePoint.

Resilience and Scalability

Multiple MaaS360 Cloud Extenders can be installed in the customer environment to provide scale and resilience. The MaaS360 Cloud is aware of all the Cloud Extender instances for a specific customer and will use them to maximize performance and reliability. The Cloud Extender provides self-monitoring and usage statistics to the MaaS360 Cloud to facilitate viewing, monitoring and alerting on Cloud Extender activity.


Microsoft Office 365
Remote PowerShell
ActiveSync (SSL:443)
MaaS360 Enabled Devices
ActiveSync (SSL:443)
Exchange Server ** 2007/2010/2013
2010/2013 TCP:80* 2007 TCP 135 TCP 49152-65535
INTERNET
DMZ
INTERNAL NETWORK
TCP:3268 TCP: 389 TCP:88 UDP:53
Active Directory/LDAP
GCM (Android)
APNs (iOS)
SSL:443
MaaS360 Cloud Extender w/ Mobile Enterprise Gateway *See CE System Requirements
Request/ Response
CSR
Certificate
Enterprise CA
Enrollment Server (NDES)
MaaS360
SSL:443
PowerShell 2.0*
Google Ports TCP/UDP: 5228 TCP/UDP: 5229 TCP/UDP: 5230
Apple Ports TCP: 5223
SharePoint
Web Servers
*Remote PowerShell by default runs on TCP port 80, most companies customize to port 443
** Server 2008
Limiting ports on Exchange 2007 http://support.microsoft.com/kb/270836

Communication Summary

Communication Path	Details
Customer Premises Cloud Extender to MaaS360 (Core Functions)	The MaaS360 Cloud Extender connects to the MaaS360 platform over TCP 443 using SSL. It requires outbound access only; it is proxy aware and keeps a connection to MaaS360 active to facilitate messaging and commands from MaaS360 to the customer's premises. Commands, data transfers and Cloud Extender monitoring, control, and updating use this connection.
Customer Premises Cloud Extender to Customer Exchange Server	The Cloud Extender communicates with the Global Catalog (Active Directory) server on port 3268. It uses the Global Catalog to figure out where the ActiveSync mailboxes are hosted. The Cloud Extender then communicates on TCP 6007 with the Exchange Mailbox server(s) to acquire ActiveSync mailbox attributes and to perform actions. It will also perform some LDAP queries on the Active Directory Server over TCP 389.

Communication Path	Details
Customer Premises Cloud Extender to Cloud Email (Office365)	The Cloud Extender communicates with the Global Catalog (Active Directory) server on port 3268. It uses the Global Catalog to figure out where the ActiveSync mailboxes are hosted. The Cloud Extender then communicates with the mailbox server(s) on Office365 to acquire ActiveSync mailbox attributes and to perform actions.
Customer Premises Cloud Extender to the Corporate Directory	For corporate directory integration, the Cloud Extender communicates with the Directory server using LDAP over TCP 389.
Customer Premises Cloud Extender to the Certificate Authority	The Cloud Extender acts as a Simple Certificate Enrollment Protocol (SCEP) relay taking certificate requests from the MaaS360 (originated from client); it interacts with the customer Certificate Authority and provides the certificate back to the MaaS360 Cloud, which will in turn complete the client request.
Customer Premises Cloud Extender Mobile Enterprise Gateway to Internal Web and Content Servers	When enabled, the Cloud Extender Mobile Enterprise Gateway module works in conjunction with the MaaS360 Cloud Relay Services to relay requests and responses between mobile applications and specific internal resources (e.g., web applications). All traffic utilizes SSL on port 443.

Enterprise Integration Details

Exchange ActiveSync 2007/2010/2013/Office 365

The Cloud Extender provides visibility into all existing devices connected to the mail system and enables auto-quarantine functionality to prevent new devices from connecting without authorization.

The Cloud Extender performs a number of functions on behalf of the MaaS360 Cloud to provide visibility and management of ActiveSync-connected devices. It:

- Queries the Exchange server using Microsoft PowerShell commands and standard APIs for information related to the ActiveSync-enabled devices. Using PowerShell and related APIs allows for abstraction from the specifics of the Exchange server implementation and allows the Cloud Extender to support multiple mailbox servers and clustered/resilient Exchange server configurations.
- Processes device and policy information, and transmits it to the MaaS360 Portal for reporting and management functions.
- Receives ActiveSync policies, actions and policy assignments, and carries out the relevant actions on the ActiveSync server.

When the Cloud Extender is configured for ActiveSync control and visibility, it performs the following activities:

- When the Cloud Extender ActiveSync module is enabled, a set of scripts runs that collects device information and ActiveSync policy information from the ActiveSync Server.
- The device and policy information collected is uploaded to MaaS360 to facilitate reporting and management workflows.
- At predetermined intervals, the Cloud Extender will look for changes in the data and policies on the ActiveSync server and any new data will be provided to MaaS360.

When the administrator requests a device action be performed on the ActiveSync server (Wipe, Policy Change, Block Approve, Remove), the action request is sent to the appropriate customer instance of the Cloud Extender and the Cloud Extender executes the requested commands on the server and returns the status to MaaS360.

Lotus Traveler ActiveSync

The Cloud Extender provides visibility into all existing devices connected to the mail system.

The Cloud Extender performs a number of functions on behalf of the MaaS360 Cloud to provide visibility of Traveler-connected devices:

- Queries Lotus Traveler server using APIs for information related to the ActiveSync-enabled devices.
- Processes device and policy information and transmits it to the MaaS360 Portal for reporting and management functions.
- Receives ActiveSync policies, actions and policy assignments and carries out the relevant actions on the Traveler server.

When the Cloud Extender is configured for ActiveSync control and visibility, it performs the following activities:

- When the Cloud Extender Lotus Traveler module is enabled, a set of scripts runs that collects device information and ActiveSync policy information from the Traveler server.
- The device and policy information collected is uploaded to MaaS360 to facilitate reporting and management workflows.
- At predetermined intervals, the Cloud Extender will look for changes in the data and policies on the Traveler server, and will provide any new data to MaaS360.

Corporate Directory for Authentication

The Cloud Extender facilitates AD/LDAP authentication:

- For self-service enrollment
- When authentication is required before accessing secured applications and documents
- When a Workplace PIN is reset by the user

The Cloud Extender receives the credentials from the MaaS360 Cloud (client originated) and validates them against the customer Directory server. The credential information is passed from the client through MaaS360 to the customer Cloud Extender, and is not persistently stored in any way.

When the Cloud Extender is configured for corporate directory authentication, it performs the following activities:

- When an authentication is required by policy, the user will be prompted to enter their Directory credentials as part of the validation process. These credentials are passed to the MaaS360 Portal.
- The credentials are then passed to the appropriate customer Cloud Extender instance.

The Cloud Extender will bind to the Directory server using the credentials provided. If the credentials are valid, the bind is successful. The Cloud Extender will send a message back to the MaaS360 Platform indicating that the credentials are good and the validation return a success.

Corporate Directory for User Visibility

The MaaS360 Cloud Extender collects Organization Units (OU), containers and user information from the corporate directory and sends the information to populate user information in the MaaS360 Cloud. This user and group information facilitates grouping for the assignment and distribution of policies, apps and docs as well as administrative role-based access.

When the Cloud Extender is configured for the corporate directory for user visibility, it performs the following actions:

- Initially, the MaaS360 Cloud Extender connects to the corporate directory and retrieves user and OU information for the configured domains, which is stored in local temporary files.
- The information in the temporary file is parsed into structured messages.
- The messages are uploaded to the MaaS360 Cloud.
- The process is repeated periodically, and changes are processed and uploaded in delta messages.

Certificate Authority

MaaS360 Certificate Services Integration allows customers to leverage their existing Microsoft or Symantec Certificate Authority (CA) and automatically provision user certificates to enrolled devices. Administrators can create email, Wi-Fi, and VPN policies & profiles that can use user-based certificates for authentication. The Cloud Extender interacts with the CA, and pushes the issued certificates down to enrolled devices.

When the Cloud Extender is configured for CA integration, it performs the following actions:

- Processes User Certificate requests from MaaS360 Cloud on behalf of mobile client requests.
- Authenticates against the CA/Registration Authority (RA) before requesting certificates.
- Issues and encrypts the user certificates and uploads them to MaaS360.
- Pushes these certificates to the requesting devices.
- Manages user certificate renewals.

BlackBerry Enterprise Server (BES)

The Cloud Extender uses the BES 5.0 Administrative APIs to provide complete visibility and control of BlackBerry devices.

When the Cloud Extender is configured for BES integration, it performs the following actions:

- Bulk registration of new devices.
- Device data query and uploads to MaaS360 from the BES for full device data or individual device attributes sets, including **Core Attributes**, **Device Heartbeat**, **Hardware Inventory—Base Data**, **Hardware Inventory—Dynamic Data**, **Network Information—Base Data**, **Network Information—Dynamic Data**, **Device Features**, **Messaging History**, **Security & Compliance**, and **Software Installed**.
- Device removal/de-registration from BES using a request.
- Query of available policies and policy upload to MaaS360.
- Facilitation of actions, including **Refresh Device Information**, **Send Message**, **Reset Device Passcode**, **Change Policy**, **Wipe Device**, and **Remove Device from BES**.
- Self-service device enrollment workflow support.

Mobile Enterprise Gateway (MEG)

The Cloud Extender can be configured provide secure mobile access to behind-the-firewall information and resources in a more efficient and targeted approach than traditional VPNs.

When the MaaS360 Cloud Extender Mobile Enterprise Gateway has been enabled and configured, the following high-level activities occur:

- The Mobile Enterprise Gateway module establishes an outbound connection to the Gateway Relay Services in the MaaS360 Cloud.
- The customer administrator defines Proxy Access List consisting of hostnames to whitelist the intranet sites allowed.
- Using one of the supported and registered MaaS360 clients (i.e., Secure Browser, Secure Documents, etc.), the user authenticates against the corporate directory and connects to the MaaS360 Cloud Relay Services via HTTPS.
- The user's application sends resource requests to the MaaS360 Relay Services, which in turn will interact with the appropriate customer Mobile Gateway to relay the requests and responses from the target customer systems.
- All traffic is AES 256 encrypted and the mobile devices never directly connect to the customer network.

Appendix A: Supporting Documentation

For more information, refer to the following:

- Cloud Extender Checklist
- Cloud Extender Installation Guide
- CERT Configuration Guide
- Mobile Enterprise Gateway Admin Guide