Citrix Endpoint Management Onboarding Handbook

Citrix Systems Netherlands BV
Spaces Zuidas, 5th floor
Barbara Strozzilaan 201
1083 HN
Amsterdam
Phone: +31 (0)20 302 3400
E-mail: info@citrix.com
Web: http://www.citrix.nl

Table of Contents

Terminology

Terminology	
Term	Definition
Customer	Refers to (customer name) and its representatives
Citrix	Refers to Citrix Systems and its representatives
MDM	Mobile Device Management
MAM	Mobile Application Management
APNS	Apple Push Notification Service
MDX	Mobile Device Experience
ADS	Discovery service
UEM	Unified Endpoint Management
SNIP	Subnet IP
NSIP	Citrix Gateway IP
VIP	Virtual IP

Introduction

Citrix Endpoint Management delivered via Citrix Cloud provides industry leading Enterprise Mobility Management (EMM) and Unified Endpoint Management (UEM) capabilities for all business types who are looking to embrace the cloud and reduce TCO for their mobile infrastructure.

Endpoint Management is an elastic pay-as-you-go SaaS subscription which allows IT to easily secure and manage mobile devices and applications while giving users the freedom to experience work and life their way. As part of a Bring Your Own Device (BYOD) program, Endpoint Management even allows end-users to use their own personal device for access to critical corporate resources.

An assisted web-based onboarding process can have Endpoint Management up and running in a matter of hours, saving IT the time and resources required to build out the infrastructure themselves. As part of the onboarding process, Endpoint Management easily integrates with on-premises enterprise systems allowing IT to quickly gain control over mobile devices and applications.

References

This document summarizes the information you need to proceed in a smooth enablement and onboarding to Endpoint Management. Use this document to record changes for your internal processes and document the service for internal references to high-level and functional designs.

Why Endpoint Management from Citrix Cloud?

1. Faster deployment. Hours instead of days.
2. No upfront cost. Minimal to no infrastructure.
3. Access to new features and bug fixes before the on-premises releases.
4. Peace of mind. 99.9% uptime.
5. No co-mingling of customer data with dedicated instances.
6. Predictable budget.
7. OpEx. Pay and get value as you go.

Endpoint Management Benefits

1. **Citrix Cloud Connector technology** provides a secure channel for communications between Citrix Cloud and your Resource Locations. This enables cloud management without requiring any complex networking or infrastructure configurations such as VPNs or IPSec Tunnels.
2. **Fully secure and redundant** channel connecting Citrix Cloud to corporate resource locations.
3. **Easy deployment** without complex infrastructure configurations.
4. **Consistency with other Citrix Cloud services**: All Citrix Cloud services including virtualized apps and desktops have standardized on Citrix Cloud Connector for enterprise connectivity delivered with a single consistent experience.
5. **Provide enterprise connectivity** to customers with strict corporate security requirements that do not allow for IPSec connectivity to cloud services.
6. **Citrix Endpoint Management MDX Security Specifics** include FIPS compliant SSL encryption for all MDX application data at rest and in transit (FIPS Citrix Gateway on-premises required).
7. **Highly available architecture** including redundant database resources and disaster recovery options for every data center.
8. **Enterprise Integration** with LDAP, PKI and certificate services to meet security and identity requirements.

Endpoint Management Features

- **Device and OS management** including iOS, Android, Android Enterprise, Windows 10, macOS, Chrome OS, Citrix Ready workspace hub, and IoT
- **Application management** including MDX, Android Enterprise, Intune App Protection, Samsung KNOX, App Configuration, and more
- **Business class mobile productivity apps** including Secure Mail, Secure Web, Citrix Files, ShareConnect, QuickEdit
- **BYOD solution** including MDM-independent MAM with no device agent requirements
- **Workspace Environment Management (WEM)** for optimized desktop application performance
- **Micro VPN** for complete application data encryption and isolation
- **Mobile SaaS** for transparent access to all managed apps
- **Microsoft Intune/EMS** app protection policies integrated with Citrix Cloud console for simple Office 365 management

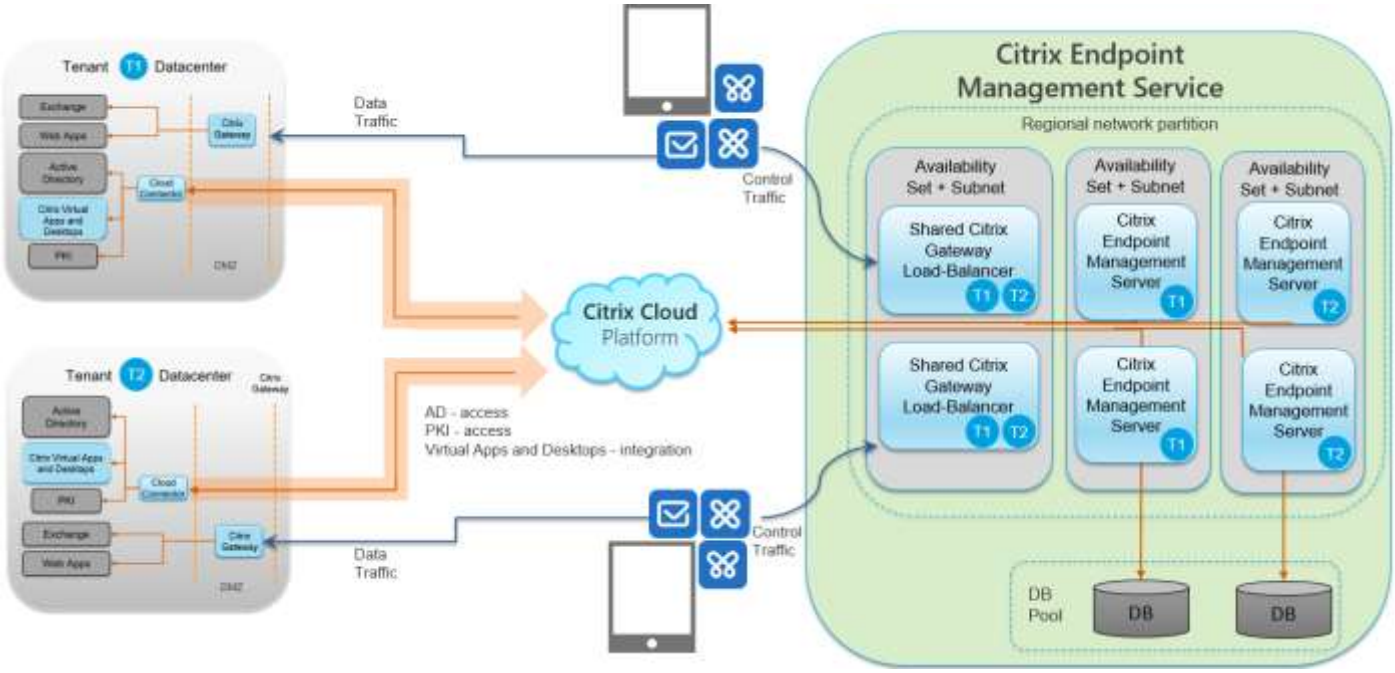
Endpoint Management compared to Workspace Premium

This information is current as of October 1, 2018. For the latest offerings, see https://www.citrix.com/products/citrix-workspace/.

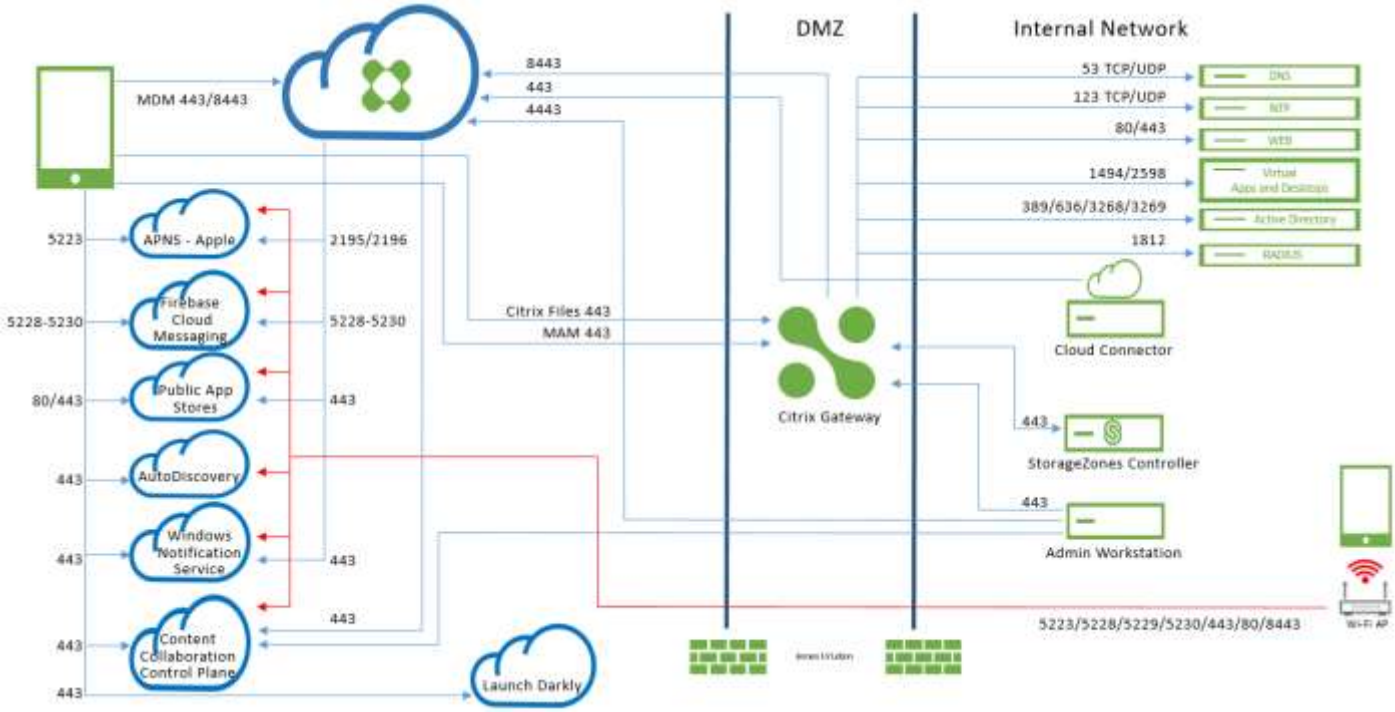
	Citrix Endpoint Management	Citrix Workspace Premium	Citrix Workspace Premium Plus*
Access via Workspace app	✓	✓	✓
Workspace Environment Management service	✓	✓	✓
Secure Unified Endpoint Management	✓	✓	✓
• Enterprise App Store	✓	✓	✓
• Mobile Device Management	✓	✓	✓
• Mobile Application Management	✓	✓	✓
• Micro-VPN	✓	✓	✓
• Citrix mobile productivity apps (Secure Mail, Secure Web, Secure Hub, QuickEdit)	✓	✓	✓
• Integration with Microsoft EMS/Intune	✓	✓	✓
Citrix Content Collaboration (ShareFile Premium - 1 TB/user*)		✓	✓
Citrix Access Control (SSO, Citrix Gateway, Cloud App Control for SaaS & Web Apps, Secure Browser, web filtering)		✓	✓
Citrix Analytics Advanced for Access Control (performance and security analytics)		✓	✓
Citrix Analytics Advanced for Workspace (performance and security analytics)		✓	✓

* Includes Citrix Virtual Apps and Desktops, not covered in this handbook.

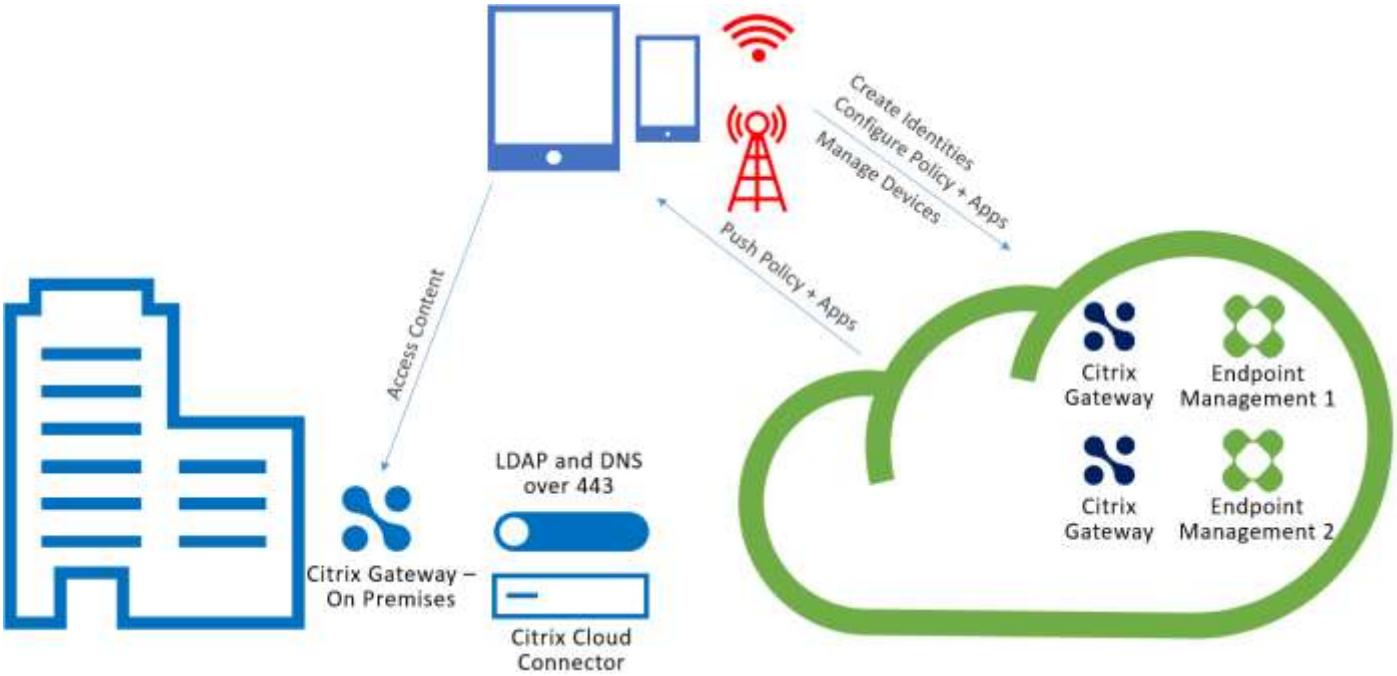
Endpoint Management High Level Architecture



Endpoint Management Traffic Flow



Endpoint Management Cloud Connector Traffic Flow



Citrix Cloud Connector Requirements

Citrix uses Cloud Connector to integrate the Endpoint Management architecture into your existing infrastructure.
For Endpoint Management in production, **a minimum availability of 2 cloud connectors is required**. In a pilot of Endpoint Management, 1 cloud connector is sufficient. Cloud Connector supports all Endpoint Management authentication types.

Server Requirements	
A dedicated physical or virtual machine	☐
Windows Server 2012 R2 or Windows Server 2016	☐
2 vCPUs	☐
4 GB RAM	☐
50 GB Hard Disk Space	☐
Active Directory Domain-Joined	☐
Domain/Forest Functional Level – 2008 R2 or Higher	☐

Platform Requirements	
.NET: .NET 4.5.1 or later	☐
Internet Connectivity	☐
Clock set to the correct UTC time	☐

Installation Requirements
You can only install the Connector onto a domain-joined machine. The installer will not allow the install to occur if it is not on a domain-joined machine.
The machine where you are installing the connector needs to be in sync with UTC time for proper installation and operation.
Switch Enhanced Security Configuration (ESC) off during installation.
Check if the required .NET version is installed. If it isn't, install the required version as described in the Citrix Cloud Connector Requirements table in this document
Copy the installer (CWCConnector.exe) to the server and run it. Make sure your browser allows the download of executable files.
You cannot install the Connector on machine templates cloned across multiple machines. Do a separate install of the Connector onto all machines.
Have outbound access to the internet through TCP port 443 (https).

For detailed technical information about Cloud Connector servers, see: https://docs.citrix.com/en-us/citrix-cloud/citrix-cloud-connector.html.

Citrix Gateway Requirements

A Citrix Gateway is required in your resource location if you require a micro VPN for either or both of the following scenarios:

- Access to internal network resources for line-of-business applications wrapped with our MDX technology and connecting to internal backend infrastructures.
- The use of Citrix mobile productivity apps, such as Citrix Secure Mail, for making email securely available to your users.

Many Endpoint Management production licenses entitle you to 2 VPX 3000 Citrix Gateways. Depending on your deployment scenario, user personas, and functional requirements, a different Citrix Gateway might be required. Contact your sales rep for additional information.

Citrix Gateway Service Requirements		
Citrix Workspace experience enabled		☐
Citrix Gateway service subscription		☐
Gateway Connector installed on-premises in a resource location		☐

Citrix Gateway Requirements (on-premises)	
New Deployment – VPX 3000 series or greater Existing Citrix Gateway deployments are supported – with a new Citrix Gateway virtual server required	☐
2 - 4 vCPUs	☐
Recommended 4 GB per vCPU	☐
20 GB Hard Disk Space	☐

Citrix Gateway Platform Requirements		
Citrix Gateway Subnet IP Address (SNIP)		☐
Citrix Gateway Management IP Address (NSIP)		☐
Citrix Gateway Internal FQDN		☐
LDAP (Active Directory) Service Account		☐

Citrix Gateway MAM Requirements		
Citrix Gateway Public IP Address (VIP)		☐
Public DNS Name – Example: http://mam.company.com		☐
Public SSL certificate 2048-bit key		☐
Proxy Load Balance IP (Internally NOT Routable – RFC1918)		☐

Citrix Gateway Requirements for Citrix Content Collaboration		
Citrix Gateway Public IP Address (VIP)		☐
Public DNS Name – Example: http://ShareFile.company.com		☐
Public SSL certificate 2048-bit key		☐
Citrix Content Collaboration Public FQDN (http://mycompany.sharefile.com)	Requested in Citrix Content Collaboration Trial	☐
Citrix Content Collaboration storage zones controller Internal IP Address		

Citrix Content Collaboration Requirements

Citrix Content Collaboration is a cloud-based file sharing service that enables users to easily and securely exchange documents. Content Collaboration enables users to send large documents by email, securely handle document transfers to third parties, and access a collaboration space from desktops or mobile devices. Content Collaboration provides users with a variety of ways to work, including a web-based interface, mobile clients, desktop tools, and integration with Microsoft Outlook.

Content Collaboration storage zones controller extends the Content Collaboration software as a service (SaaS) cloud storage by providing your Content Collaboration account with private data storage.

Content Collaboration Storage Zones Controller Requirements		
A dedicated physical or virtual machine		☐
Windows Server 2012 R2 or Windows Server 2016		☐
2 vCPUs		☐
4 GB		☐
50 GB Hard Disk Space		☐

Content Collaboration Storage Zones Controller Server Role Requirements		
Web Server (IIS)		☐
Application Development: ASP.NET 4.5.2		☐
Security: Basic Authentication		☐
Security: Windows Authentication		☐

Content Collaboration Platform Requirements		
The Citrix Files app installer requires administrative privileges on the Windows Server		☐
Content Collaboration Admin User name		☐

Customer Infrastructure Components

When implementing an Endpoint Management infrastructure with secure connectivity to your internal network: The Citrix Gateway on-premises and Endpoint Management in the Cloud need to communicate with the internal network resources listed in the below table. You can record your information in the following table for reference during the preparation, onboarding, and Pilot phases.

Infrastructure Components Reference Table		
DNS Server IP Address		☐
DNS Server FQDN		☐
Proxy Server for Outgoing Traffic		☐
Proxy Authentication needed?	Yes/No	☐
Proxy Server for Incoming Traffic		☐

Proxy Authentication needed?	Yes/No	☐
Active Directory Server Internal IP Address		☐
Active Directory Server Internal FQDN		☐
Active Directory Server Port		☐
AD Server SSL Certificate – max 2048-bit key		☐
Active Directory Domain Name		☐
Active Directory User Base DN		☐
Active Directory Search User ID		☐
Active Directory Search User Password is known and tested		☐
SMTP Server External IP		☐
SMTP Server External FQDN		☐
SMTP Server Port		☐
SMTP Relay User name (if needed)		☐
SMTP Relay User Password is known and tested (if needed)		☐
Exchange Internal IP Address		☐
Exchange Internal FQDN		☐
Exchange Server Port		☐
Exchange Server SSL Cert – max 2048-bit key		☐
SharePoint Server Internal IP (if needed)		☐
SharePoint Server Internal FQDN		☐
SharePoint Server Port		☐
All FQDNs are tested, including reverse lookup	Yes/No	☐

Network and Firewall Requirements

To enable devices and apps to communicate with Endpoint Management, you open specific ports in your firewalls. The following tables list the ports that must be open.

Open ports from Internal Network to Citrix Cloud					
TCP port	Description	Source IP	Destination	Destination IP	
443	Cloud Connector		https://*.citrixworkspacesapi.net https://*.cloud.com (commercial) https://*.cloud.us (government) https://*.sharefile.com https://cwsproduction.blob.core.windows.net/downloads https://*.servicebus.windows.net		☐
4443	Administrative Console		https://*.citrixworkspacesapi.net https://*.cloud.com (commercial) https://*.cloud.us (government) https://*.citrix.com https://*.blob.core.windows.net		☐

Open ports from Internet to DMZ					
TCP port	Description	Source IP	Destination	Destination IP	
443	Endpoint Management Client Device		Citrix Gateway IP		☐
443	Endpoint Management Client Device		Citrix Gateway VIP Content Collaboration		☐
443	Content Collaboration Public IP	CTX208318	Citrix Gateway VIP Content Collaboration		☐
443	StoreFront		Citrix Gateway IP		☐

Open ports from DMZ to Internal					
TCP port	Description	Source IP	Destination	Destination IP	
389 or 636	Citrix Gateway NSIP (or, if using a load balancer, SNIP)		LDAP/Active Directory IP		☐
53 (UDP)	Citrix Gateway SNIP		DNS Server IP		☐
443	Citrix Gateway SNIP		Exchange (EAS) Server IP		☐
80/443	Citrix Gateway SNIP		Internal Web Apps/Services		☐
443	Citrix Gateway SNIP		Content Collaboration Storage Zones Controller IP		☐
123	Citrix Gateway SNIP		NTP server		☐
1494	Citrix Gateway SNIP		Virtual Apps and Desktops		☐
1812	Citrix Gateway NSIP		RADIUS Authentication Server		☐
2598	Citrix Gateway SNIP		Virtual Apps and Desktops		☐
3268	Citrix Gateway NSIP		Secure Global Catalog Server		☐
3269	Citrix Gateway NSIP		Global Catalog Server		☐

Open ports from Internal to DMZ					
TCP port	Description	Source IP	Destination	Destination IP	
443	Admin Client		Citrix Gateway NSIP		☐

Open ports from DMZ to Internet					
TCP port	Description	Source IP	Destination	Destination IP	
8443	Citrix Gateway SNIP		Endpoint Management Cloud		☐
443	Citrix Gateway		Launch Darkly		☐

Open ports from Internal to Internet					
TCP port	Description	Source IP	Destination	Destination IP	
443	Exchange (EAS) Server IP		Endpoint Management Push Notification Listener (us-east-1.mailboxlistener.xm.citrix.com) (eu-west-1.mailboxlistener.xm.citrix.com) (ap-southeast-1.mailboxlistener.xm.citrix.com)		☐
443	Content Collaboration Storage Zones Controller IP		Content Collaboration Control Plane	CTX208318	☐

Open ports from Corporate Wi-Fi to Internet					
TCP port	Description	Source IP	Destination	Destination IP	
5223	Endpoint Management Client Device		Apple APNS Servers	17.0.0.0/8	☐
5228	Endpoint Management Client Device		Firebase Cloud Messaging	android.apis.google.com, cm.googleapis.com	☐
5229	Endpoint Management Client Device		Firebase Cloud Messaging	android.apis.google.com, cm.googleapis.com	☐
5230	Endpoint Management Client Device		Firebase Cloud Messaging	android.apis.google.com, cm.googleapis.com	☐
443	Endpoint Management Client Device		Windows Push Notification Service	*.notify.windows.com	☐
443 / 80	Endpoint Management Client Device		Apple iTunes App Store	ax.itunes.apple.com *.mzstatic.com vpp.itunes.apple.com	☐
443 / 80	Endpoint Management Client Device		Google Play	play.google.com, android.clients.google.com, android.l.google.com, android.com, google-analytics.com	☐
443	Endpoint Management Client Device		Firebase Cloud Message	cm.googleapis.com	☐

443 / 80	Endpoint Management Client Device		Microsoft App Store	login.live.com, *.notify.windows.com	☐
443	Endpoint Management Client Device		Endpoint Management discovery service	ads.xm.cloud.com (Secure Hub versions supported as of January 1, 2019)	☐
8443 / 443	Endpoint Management Client Device		Endpoint Management		☐
443	Content Collaboration Storage Zones Controller IP		Content Collaboration Control Plane	CTX208318	☐
443	Endpoint Management Client Device		Google Mobile Management, Google APIs, Google Play Store APIs	*.googleapis.com	☐
443	Endpoint Management Client Device		Connectivity check prior to CloudDPC v470. Android connectivity check starting with N MR1 requires for https://www.google.com/generate_204 to be reachable, or for the given Wi-Fi network to point to a reachable PAC file)	connectivitycheck.android.com, www.google.com	☐

Network requirements for Android Enterprise

For more information on Android Enterprise network and port requirements, see https://docs.citrix.com/en-us/citrix-endpoint-management/system-requirements.html#android-enterprise-network-requirements

Port requirement for discovery service connectivity
This port configuration ensures that Android devices connecting from Secure Hub for Android can access the Citrix discovery service from within the internal network. The ability to access the discovery service is important when downloading any security updates made available through the discovery service.

Note: ADS connections might not support your proxy server.
In this scenario, allow the ADS connection to bypass the proxy server.

Port requirements for Citrix Gateway

For more information on Citrix Gateway port requirements, see https://docs.citrix.com/en-us/citrix-endpoint-management/system-requirements.html#citrix-gateway-port-requirements

Certificate Pinning Prerequisites
If you want to enable certificate pinning, complete the following prerequisites:

- Collect Endpoint Management server and Citrix Gateway certificates. The certificates must be in PEM format and must be a public certificate and not the private key.
- Contact Citrix Support and place a request to enable certificate pinning. During this process, you are asked for your certificates.

Certificate pinning requires that devices connect to discovery service before the device enrolls. This requirement ensures that the latest security information is available to Secure Hub. For Secure Hub to enroll a device, the device must reach the discovery service. Therefore, opening the discovery service access within the internal network is critical to enabling devices to enroll.

To allow access to the discovery service for Secure Hub for Android, open port 443 for the following FQDN and IP addresses:

Port requirement for discovery service connectivity			
FQDN	IP Address	Port	IP and Port Usage
ads.xm.cloud.com (Secure Hub versions supported as of January 1, 2019); (discovery.mdm.zenprise.com (Secure Hub 10.6.15 and older)	52.5.138.94	443	Secure Hub - ADS Communication
ads.xm.cloud.com (Secure Hub versions supported as of January 1, 2019); (discovery.mdm.zenprise.com (Secure Hub 10.6.15 and older)	52.1.30.122	443	Secure Hub - ADS Communication
ads.xm.cloud.com	34.194.83.188	443	Secure Hub - ADS Communication
ads.xm.cloud.com	34.193.202.23	443	Secure Hub - ADS Communication

Google/Apple/Microsoft Requirements

Apple		
Apple Push Certificate	http://identity.apple.com	☐

Google		
Google Play Account	https://accounts.google.com/signup	☐
Google Play Device ID	http://docs.citrix.com/en-us/endpoint-management/provision-devices/google-play-credentials.html On a device with no sim (dial pad), install the Device ID app: https://play.google.com/store/apps/details?id=com.redphx.deviceid	

Microsoft		
Windows Store developer account	https://msdn.microsoft.com/en-us/library/windows/apps/jj863494.aspx	☐
Windows Store Publisher ID.	https://msdn.microsoft.com/en-us/library/windows/apps/hh967786.aspx	☐
Enterprise certificate from Symantec	https://msdn.microsoft.com/library/windows/apps/jj206943.aspx	☐
Public SSL certificate for discovery service	http://docs.citrix.com/en-us/endpoint-management/provision-devices/autodiscovery.html	☐
Application Enrollment Token (AET)	https://msdn.microsoft.com/en-us/library/windows/apps/jj735576%28v=vs.105%29.aspx	☐

For more detailed information on the supported mobile platforms for Endpoint Management, see https://docs.citrix.com/en-us/citrix-endpoint-management/system-requirements/supported-device-platforms.html

Deployment Use Cases

Below are the various deployment use cases which are feasible with Endpoint Management.

Citrix Endpoint Management and Citrix Gateway on Enterprise
Citrix Endpoint Management and Citrix Gateway on Enterprise for Mobile App Management
Citrix Endpoint Management and Citrix Gateway on Enterprise for Mobile App Management with Citrix Content Collaboration for Enterprise File Sharing
Citrix Endpoint Management for Mobile Devise Management

For more detailed information on the deployment use cases, see the Citrix Support Article https://support.citrix.com/article/CTX223709 or this white paper: https://citrix.sharefile.com/d-sba63ccb1290430ca.

Deployment Scenarios

Scenario	Use Case Example
Citrix Endpoint Management	BYOD or company issued Medium Security/privacy requirements Native or Secure email View/edit email attachments Already have a solution for EFSS Need secure off-the-shelf apps Looking into developing own mobile apps -or- Company owned, shared device “Kiosk,” for example, an iPad used by warehouse workers for inventory
Workspace Premium	BYOD or company issued High security/privacy requirements Secure email View/edit email attachments Need to solve EFSS Need secure off-the-shelf apps Need to secure several internally developed mobile apps Can’t store any data on mobile device

Endpoint Management MDM Pilot Test Cases Example

This section lists example test cases and categories specific to device management. The test results should be recorded here for future reference and audit purposes.

Pilot MDM Test Matrix

Secure Hub Version	iOS =	Android=	Windows=
Endpoint Management Version	10.x		
Citrix Gateway Version	10.x		

Test Cases	Category	Expected Result	Result	
From Secure Hub, enroll using an Enrollment URL Invitation and a one-time PIN number From Secure Hub, enroll to the XM Service using Active Directory credentials	Enrollment	The ability to use a unique URL to enroll into the system without requiring AD credentials	☐	☐
		The ability to enroll into Endpoint Management and have policies and profiles sent down automatically	☐	☐
		The ability to use a single app on each platform to enroll and subsequently control MDM policies	☐	☐
Via the XM Service Administration console, define and deploy policies that will secure the device	Security Policies	The ability to provision security policies, such as enforcing a passcode and setting restrictions	☐	☐
Via the XM Service Administration console, define and deploy policies that will aid the user and simplify the configuration of the device	Provisioning Policies	The ability to provision Wi-Fi, VPN, Email and Proxy policies	☐	☐
		The ability to issue certificates to the device, including user-based certificates that can be used as credentials	☐	☐
		The ability to deliver apps (in-house or from a public App Store) to the device.	☐	☐
Via the XM Service Administration console, understand the current state of a device	Operational Supportability/ Administration	The ability to determine device status, inventory, software inventory and MDM policy deployment status	☐	☐
		The ability to locate devices	☐	☐
Test the support functionality within Secure Hub	Support	The ability to use Secure Hub to determine why the device might be out of compliance	☐	☐
		The ability to automatically collect logs from the device and send to the helpdesk	☐	☐
		The ability to initiate a live chat session with a helpdesk operator	☐	☐
Via the XM Service Administration console, remotely de-provision devices	De-provisioning	The ability to perform a selective wipe remotely and to remove from the device the provisioned policies, apps and data	☐	☐
		The ability to perform a full wipe (factory reset)	☐	☐
		The ability to revoke a device to remove the provisioned profiles, apps and data and prevent the device from being enrolled again	☐	☐

Citrix mobile productivity apps/MDX Pilot Test Cases Example

This section lists example test cases and categories specific to device management. The test results should be recorded here for future reference and audit purposes.

Pilot Citrix mobile productivity apps /MDX Test Matrix

Secure Hub Version	iOS =	Android=	Windows=
Endpoint Management Version	10.x		
Citrix Gateway Version	10.x		

Test	Success Criteria	iOS		Android		Win10	
Post Enrollment Gateway Logon	When Secure Hub 'flips' from enrollment to Citrix Gateway, the user should not need to re-enter credentials	☐	☐	☐	☐	N/A	N/A
Citrix PIN Creation	User should be prompted to create a 6-digit Citrix PIN	☐	☐	☐	☐	N/A	N/A
Endpoint Management app store	User can access Endpoint Management app store from within Secure Hub and is entitled to Secure Web, Secure Mail, Secure Tasks, Secure Edit, Secure Notes and Citrix Files	☐	☐	☐	☐	N/A	N/A
Secure App Installs	Secure Web, Secure Mail, Secure Tasks, Secure Edit, Secure Notes and Citrix Files can all be installed	☐	☐	☐	☐	N/A	N/A
Collect Secure Hub Logs	Swipe right within Secure Hub to the Support Page and then tap Secure Hub	☐	☐	☐	☐	N/A	N/A
Inactivity Timer <15 Minutes	Launch Secure Web and authenticate if required. Leave device unattended for 10 minutes, then attempt to access Secure Web. Secure Web should open without requiring Citrix PIN	☐	☐	☐	☐	N/A	N/A
Inactivity Timer >15 Minutes	Launch Secure Web and authenticate if required. Leave device unattended for 18 minutes, then attempt to access Secure Web. Secure Web should prompt for Citrix PIN before opening.	☐	☐	☐	☐	N/A	N/A
MDX App Wipe	After admin sends an MDX App Wipe command via the console, user data is removed from all Citrix mobile productivity apps	☐	☐	☐	☐	N/A	N/A