Using CAPTOR for MobileIron v3.5.x

October 31, 2019
Proprietary and Confidential
Do Not Distribute

What's New?

- New policy to add a watermark on photos and documents

Overview

CAPTOR™ is an AppConnect app enabling secure content capture for government and enterprise customers, effectively combining four apps in one - camera, document scanner, audio recorder, and QR code reader - with military grade encryption, IT policy controls, and separation of business and personal content to support BYOD/COPE.

App availability

CAPTOR for MobileIron (iOS AppConnect):

Bundle ID: com.inkscreen.photoink.mobileiron

App Store: https://itunes.apple.com/us/app/captor-for-mobileiron/id936292792?ls=1&mt=8

Device Compatibility

The app supports all 64-bit iOS devices (iPhone and iPad) released since 2013.

App-Specific Configuration

Key	Description	Default if not configured
licensekey	License key for use of application used to determine and track number of devices provisioned. **IMPORTANT:** The application must be able to reach https://api.backendless.com/ in order to authenticate the license. Please check firewall settings to ensure devices can reach this domain. **REQUIRED FOR ACTIVATION**	CAPTOR will only work in unencrypted PIN-mode if the appropriate license key is not added
captoruser	Links the username field within the app to either the email address or user ID for that user as listed in MobileIron Core. The app user will not be able to change the app username once this key-pair is set. The MobileIron admin can change this value any time without negatively impacting users. Value entered should be either $USERID$ or $EMAIL$. Please note: the username can be displayed on the photo or video as a caption, and inserted as metadata. **REQUIRED FOR ACTIVATION**	If key-value pair is not configured, the app will not be able to authenticate against the license server.

filenamebase	Sets a base name for photos, videos, and documents captured with the app. The nomenclature system appends the base with a sequential number starting with 000 (ex. CAPTOR000.JPG). Value can be an alpha-numeric string 1-20 characters with no spaces, or $USERID$ **ADDING THIS KEY-VALUE PAIR IS HIGHLY RECOMMENDED**	If key-value pair is not configured, the default filename base will be CAPTOR and the user can edit.
allowemail	Enables or disables the use of the native iOS email client. Value entered should be either true or false. Also required to set the Container Policy for Allow Open In to the "whitelist" option, and include the following two bundle IDs: com.apple.UIKit.activity.Mail com.apple.mobilemail Note 1: If you use Email+ or any other non-native email app, these options will appear in the Open In menu. Note 2: At this time, MobileIron does not support the sharing of content between AppConnect apps and the native iOS Email app for customers using MobileIron Cloud.	If key-value pair is not configured, the default is to disable the ability to share using the native email app.
videotimelimit	Enables or disables the ability to capture video. To disable video capture completely, enter a value of 0. To enable video capture, enter a whole number 1 - 9999 representing the maximum length a video can be recorded in seconds.	If key-value pair is not configured, video capture will be enabled with a maximum capture length of 999 seconds.
allowimport	Enables or disables the ability to bring photos and videos into CAPTOR from the native media gallery. Value entered should be either true or false.	If key-value pair is not configured, importing media will not be allowed.

emptytrash	Sets a value (in days) to wait before permanently deleting media content that a user has moved to the Trash folder in the app. Value entered should be a whole number 0 - 999. Entering "0" means the Trash folder will be emptied each time the app is launched.	If key-value pair is not configured, the default setting is to delete contents of the Trash folder that are older than 30 days.
localization	Sets the language to be one of the five supported currently by CAPTOR. Value entered is the two character abbreviation for the language setting. Current options include: en = English es = Spanish fr = French de = German it = Italian nl = Dutch	If key-value pair is not configured, the default localization setting will be English (en).
showcaption	Enforces the printed caption on the border of photos, and the addition of a final frame to shared videos. The caption includes 1) username of who captured the media, 2) time and date of capture, 3) location where media was captured (lat/long or city/state/country), and a note (up to 255 char). Value entered should be TRUE or FALSE, whereby TRUE dictates the caption will always be included and FALSE removes the caption in all cases. Please note: this feature does not impact Documents or Audio.	If key-value pair is not configured, the user will have the ability to set the caption on or off in the app Settings.

browserscheme	Sets the default web browser so that any links accessed from the app launch the desired web browser. Value entered may be one of the following (only enter the bold text): **mibrowser://** (Web@Work HTTP) **mibrowsers://** (Web@Work HTTPS) **googlechrome://** (Google Chrome) Please note: If none of the supported browsers are present on the device, Safari will be used.	If key-value pair is not configured, the default browser is Safari.
pdfversion	Sets the version of PDF that will be created when sharing documents or photos in the PDF file format. Value entered may be: 1.3 1.4 1.5 1.6 1.7 PDF/A-1a PDF/A-1b PDF/A-2a PDF/A-2b PDF/A-2u PDF/A-3a PDF/A-3b PDF/A-3u	If key pair is not configured, the default will be 1.3 and the user will be able to adjust. *If set to any of the PDF/A subtypes, the option to set a PDF password will be disabled.
allowlocation	Determines whether the application will prompt to allow location services and tag media with location information. Values entered may be: user (allows user to decide whether to enable location services) false (completely disables all location services)	If key pair is not configured, the default will allow the user to accept or deny location services.

filesizelimit	Sets the maximum size of a shared file (in MB). Values entered may be 1 - 30.	If key pair is not configured, the default will be “unlimited”, allowing the user to attempt to share files of any size.
watermark	Adds a semi-transparent watermark across photos and document pages. 30 character limit. Supports $USERID$ and $EMAIL$ wildcard values, or custom strings.	If key pair is not configured, the default is to allow the user to enter their own watermark if desired.

Secure Content Copy Backup Service

Secure Content Copy is an optional service enabling the backup of CAPTOR content to a server or network drive.

Before setting up the service, you must establish a server on your network to receive the content. Additionally, the server must be configured to include folders for each CAPTOR user which can be mapped to. If you utilize the key "captoruser" with value $USERID$, the folders on your backup server should be named the same way.

We recommend using MobileIron Sentry and AppTunnel to secure the data traffic and entry into your corporate network.

Here is an overview of the process to set up the backup service:

1) Select the best data transfer protocol. CAPTOR currently supports SMB2, SFTP, Microsoft OneDrive, and WebDAV. **The SMB protocol requires the use of a VPN (ex. MobileIron Tunnel App, Cisco AnyConnect).

2) Establish a server on your network to receive the content. Create folders for each user, named to match the CAPTOR usernames.

3) Create a MobileIron Sentry and AppTunnel to encrypt and control the traffic into your network from the CAPTOR app.

4) Establish the key/value pairs in Core or Cloud to enable and configure the service. At a minimum, you must enter "enablebackup" with the value matching your selected data transfer protocol.

5) Launch CAPTOR on a test device and review the configuration by going to Settings>Backup Config. Depending on your configuration you may have to complete the settings for the selected transfer protocol and/or Advanced Config options.

6) Test Configuration: There is a button to test the configuration in each transfer protocol screen. If the backup process runs successfully you will see an alert indicating success. If there is a failure of any kind, you will receive one of the following alerts:

- Could not reach server (09)
- Could not connect to server (19)
- Could not open directory at path (29)

- Invalid SFTP host or port (39)
- Invalid SMB share (49)
- Invalid WebDAV URL (59)
- Invalid SMB host (69)
- Directory not found at path (79)
- The request timed out (89)
- Unauthorized: Bad username or password (99)

The following key/value pairs can be added to the AppConnect Configuration.

Key	**Description**	**Default if not configured**
enablebackup	This is the master switch to turn on the backup service. The value entered identifies which transfer protocol will be used. Only one protocol can be established at a time, so the remaining protocols will be disabled. Values entered may be: webdav sftp smb onedrive	If key pair is not configured, the backup service will be disabled.
backupmethod	The backup process can be automated, or allowed to be conducted by the user on demand. Values entered may be: auto manual	If key pair is not configured and enable backup is configured, the default will be manual.
automatebackupafter	If you intend the backup process to be automated, this key is required. The value entered indicates how long the system will wait before backing up content. For example, setting a value "7" means that the system will backup content that was captured at least 7 days prior. Entering a value "0" will backup content in the next user session. Values entered may be 0-30.	If key pair is not configured and backupmethod is set to "auto", the default will be 1.

deletebackedupafter	When configured this will move backed-up content to the CAPTOR Trash folder after a specified number of days after it was backed up. For example, a value "3" would instruct the system to trash an item three days after it was backedup. A value "0" instructs the system to trash items immediately after backup. Values entered can be 0-30.	If key pair is not configured, the default is set to never delete content after it is backedup.
contentquality	Sets the quality of the content that is backedup. The system uses the same quality standards as the normal sharing options . Values entered maybe: low med high	If key pair is not configured, the default is high.

Backup Protocol Key/Value Pairs

The next step is to set the key pairs related to the backup transfer protocol that you selected. You may only use one protocol for any specific label. Please select one protocol (WebDAV, SMB, or SFTP) and then enter the corresponding key/value pairs into the configuration.

WebDAV

Key	**Description**	**Default if not configured**
webdavuser	Assigns the username for authentication of backup server. For most customers the value entered should be $USERID$	If key pair is not configured, the user will be allowed to set the username within the app.

webdavpassword	Assigns the password for authentication of backup server. For most customers the value entered should be $PASSWORD$.	If key pair is not configured, the user will be allowed to set the password within the app.
webdavurl	Assigns the URL to the backup server. Value entered should be a valid url; for example "https://23-22.companynet.com"	If key pair is not configured, the user will be allowed to set the URL within the app.
webdavpath	Assigns the directory path for the user's folder on the backup server. *Please note, the user folders must be created on the server by the IT Admin prior to setting this configuration. For most customers, the value entered should be: /$USERID$/	If key pair is not configured, the user will be allowed to set the path within the app.

SMB

**SMB requires a VPN (ex. MobileIron Tunnel App, Cisco AnyConnect) for all situations except transferring files over a local network.		
Key	**Description**	**Default if not configured**
smbhost	Assigns the IP address for the backup server.	If key pair is not configured, the user will be allowed to set the host within the app.
smbuser	Assigns the username for authentication of backup server. For most customers the value entered should be $USERID$	If key pair is not configured, the user will be allowed to set the username within the app.

smbpassword	Assigns the password for authentication of backup server. For most customers the value entered should be $PASSWORD$.	If key pair is not configured, the user will be allowed to set the password within the app.
smbshare	Assigns the SMB share name. This field may not be required for all implementations.	If key pair is not configured, the user will be allowed to set the share within the app.
smbpath	Assigns the directory path for the user's folder on the backup server. *Please note, the user folders must be created on the server by the IT Admin prior to setting this configuration. For most customers, the value entered should be: $USERID$	If key pair is not configured, the user will be allowed to set the path within the app.

SFTP

Key	**Description**	**Default if not configured**
sftphost	Assigns the IP address or URL for the backup server.	If key pair is not configured, the user will be allowed to set the host within the app.
sftpuser	Assigns the username for authentication of backup server. For most customers the value entered should be $USERID$	If key pair is not configured, the user will be allowed to set the username within the app.

sftppassword	Assigns the password for authentication of backup server. For most customers the value entered should be $PASSWORD$.	If key pair is not configured, the user will be allowed to set the password within the app.
sftpport	Assigns the network port. Value entered should be numeric (for example: 22).	If key pair is not configured, the user will be allowed to set the port within the app.
sftppath	Assigns the directory path for the user's folder on the backup server. *Please note, the user folders must be created on the server by the IT Admin prior to setting this configuration. For most customers, the value entered should be: /$USERID$	If key pair is not configured, the user will be allowed to set the path within the app.
sftpsshpassphrase	Only for SFTP implementations utilizing SSH2/RSA keys. This field assigns the SSH Key Passphrase. Not all SSH Key implementations will require this key.	If key pair is not configured, the user will be allowed to enter the value within the app.
sftpsshkey	Only for SFTP implementations utilizing private SSH2/RSA keys. This field would contain the actual text of the key. Most situations require the end user to copy and paste the key into the app.	If key pair is not configured, the user will be allowed to enter the value within the app.

OneDrive

**Implemented with MSAL and requires ADFS 2019		
Key	**Description**	**Default if not configured**
onedrivepath	Assigns the directory path for the user's folder. *Please note, the user folders must be created on the server by the IT Admin prior to setting this configuration.	If key pair is not configured, the user will be allowed to set the path within the app.

Data Loss Prevention Policy Support

CAPTOR supports the following DLP components:

- the pasteboard DLP policy
- the Open In DLP policy

Secure File I/O Support

Yes, CAPTOR provides secure file I/O support.

AppConnect & Non-AppConnect Mode Support

CAPTOR for MobileIron will function as an AppConnect-enabled app or in an unencrypted PIN-mode. If you need to test CAPTOR in unencrypted PIN-mode, please email support@inkscreen.com to request a PIN.

Features

CAPTURE

- **Photos:** capture and annotate high resolution photos
- **Videos:** record and edit short videos
- **Documents:** Scan paper documents to PDF

- **Audio:** record ambient audio
- **QR:** snap a QR code to translate URL and launch browser
- Apply annotations such as text labels, drawings, or arrows
- Caption with time/date, GPS location, username, and notes

MANAGE
- Control resolution & quality when sharing to manage file size
- Store content separate from personal photo galleries (BYOD or COPE)
- Import content to CAPTOR (based on policy)
- Share via policy approved apps

SECURE
- All captured content and associated data is encrypted
- Granular IT policies to enforce sharing, importing, file management, etc
- Remotely erase content if a device is lost or stolen

CAPTOR for MobileIron landing page: http://www.inkscreen.com/mobileiron

For More Information

CAPTOR for MobileIron End User Getting Started Guide: https://inkscreen.freshdesk.com/support/solutions/articles/1000255749-captor-for-mobileiron-3-x-getting-started-guide

Request a trial license key: www.inkscreen.com/trial

ATTENTION: The next section of documentation is specific to MobileIron Core implementations. If your organization utilizes MobileIron Cloud, please skip to page 16.

MobileIron Core Configuration Tasks

Use the following high-level steps to configure AppConnect for the app.

1. Enable AppConnect.

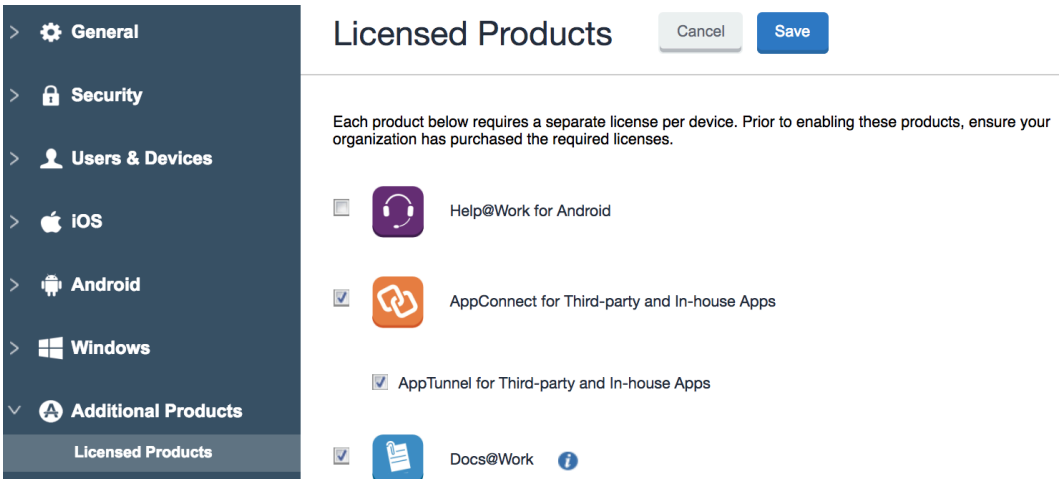
2. Configure an AppConnect global policy.

3. Configure a new AppConnect app configuration for the app.
4. Configure a new AppConnect container policy for the app.
5. Assign Labels to both the app configuration and the app container policy.

Enable AppConnect

Before enabling AppConnect on your VSP, confirm that your organization has purchased the required AppConnect licenses. Contact your MobileIron representative if you require additional details on AppConnect license purchases.

To enable AppConnect and AppTunnel functionality on the VSP, navigate to the Settings page on the VSP Admin Portal and check the boxes as shown below.



1. Select the option for "Enable AppConnect for third-party and in-house apps".
2. Select the option of "Enable AppTunnel for third-party and in-house apps".

Configure an AppConnect Global Policy

An AppConnect global policy configures the security settings for all AppConnect apps, including:

- Whether AppConnect is enabled for the devices that the policy is applied to
- AppConnect passcode requirements.

  Note: The AppConnect passcode is not the same as the device passcode.
- out-of-contact timeouts
- the app check-in interval

  Note: The app check-in interval is independent of the MDM check-in timer and controls, and apps cannot be forced to check-in before the interval expires. The recommended configuration for the app check-in interval is 60 minutes.
- the default end-user message for when an app is not authorized by default
- whether AppConnect apps with no AppConnect container policy are authorized by default
- data loss prevention settings

To modify an existing AppConnect global policy:

1. On the VSP Admin Portal, go to Policies & Configs > Policies.
2. Select an AppConnect global policy.
3. Click Edit.
4. Edit the AppConnect global policy based on your requirements.

   See the AppConnect chapter of the VSP Administration Guide for details about each field.

Configure a New AppConnect App Configuration

The AppConnect app configuration defines the app-specific parameters that are automatically pushed down to the app, as well as configurations for establishing

and authenticating an AppTunnel associated with the app. See the AppConnect chapter of the VSP Administration Guide for details about each field.

Also, for more on AppTunnel configuration, see "Adding AppTunnel Support" in the AppConnect chapter of the VSP Administration Guide.

Use the following steps to configure the app-specific configuration:

1. On the VSP Admin Portal, go to Policies & Configs > Configurations > Add New > AppConnect > Configuration.

2. Edit the AppConnect app configuration with the Name, Description, Application, and App-specific key-value pair configurations required for the app.

   Note: For the Application field, choose an application from the app distribution library, or for iOS apps, specify the iOS bundle ID. You can find the bundle ID by going to Apps > App Distribution Library, and clicking to edit the app. The field Inventory Apps displays the bundle ID in parenthesis.

3. App Specific Configuration: Click on the "+" button to enter the key-value pair information.

Configure a New AppConnect Container Policy

An AppConnect container policy specifies data loss protection policies for the app. The AppConnect container policy is required for an app to be authorized unless the AppConnect global policy allows apps without a container policy to be authorized. Such apps get their data loss protection policies from the AppConnect global policy.

Details about each field are in the AppConnect chapter of the VSP Administration Guide.

To configure an AppConnect container policy:

1. On the VSP Admin Portal, go to Policies & Configs > Configurations > Add New > AppConnect > Container Policy.

2. Enter the Name, Description, and Application.

   Note: For the Application field, choose an application from the app distribution library, or for iOS apps, specify the iOS bundle ID. You can find the bun-

dle ID by going to Apps > App Distribution Library, and clicking to edit the app. The field Inventory Apps displays the bundle ID in parenthesis.

3. Configure the data loss protection policies according to your requirements.

Apply Labels

Please ensure that you have applied a Label to both the configuration policy and the container policy. The Label should identify the device or set of devices intended to be configured to use the app.

This concludes the instructions for setting up CAPTOR in a MobileIron Core environment

MobileIron Cloud Configuration Tasks

This section of instructions is specific to MobileIron Cloud environments.

Add CAPTOR for MobileIron to Apps

Enter the Apps section and click "+Add". In the search field, enter "CAPTOR for MobileIron". Click on the app icon to highlight the listing, and click "Next". You will be given an option of pushing the app to all users or a subset of users.

AppConnect Custom Configuration

You will be presented next with a main section titled App Configurations. Scroll down to AppConnect Custom Configuration and click + to add.

In the Configuration Setup, you are required to give the configuration a name. Next, add the key "licensekey" and enter the key value provided by Inkscreen. Then add the key "captoruser", and most customers will use the value $USERID$. Continue by adding any additional key/value pairs that are relevant for your business (see list starting on page 2). Click Next, and then Done to finalize the configuration.