Colligo Briefcase

for Good Technology

Administrator Guide

Contents

Introduction

This document provides guidance for your deployment of Colligo Briefcase for Good Technology, herein referred to as simply Colligo Briefcase. Colligo Briefcase Pro and Lite editions are available through the App Store and are not covered by this document.

User documentation is available on the Colligo support website at http://www.colligo.com/support/

For any further technical details, please contact Colligo Technical Support at support@colligo.com, or for sales related questions, please contact sales@colligo.com.

Target Audience

- IT Administrators
- Technical Evaluators
- Deployment Managers

Overview

Colligo Briefcase lets you easily store, sync, view and find SharePoint content on your iPad, iPhone or iPod Touch. You can access and share files, lists, images, documents, and emails. Synchronize SharePoint content to your devices automatically, for instant access, even when offline as well as create, edit, or modify documents for automatic upload to SharePoint when back online. Confidently support iPads, iPhones, or iPod Touches in your enterprise with security features designed to ensure the integrity of your corporate data.

Colligo Briefcase works with every Colligo email management solution for desktops, laptops, and smartphones, providing unified, centrally-managed access to SharePoint content, online and off, on-premise or in the cloud.

Key Features

- View SharePoint files directly on your mobile device, including Office (Word, Excel, Outlook, PowerPoint) documents, PDFs, images, emails and more
- Keep SharePoint content offline for fast access, even when you are not on the network
- Share files easily using links
- Find your content fast with powerful search
- Open and edit files in applications such as Documents to Go or GoodReader
- Upload files and photos to SharePoint
- View and edit document and file properties, including metadata
- Enter and submit InfoPath forms, with support for signatures
- Secure access to Briefcase using passcode protection

Platforms Supported

- iPad (2nd generation and higher), iPad Mini, iPhone (3GS and above), iPod Touch (4th generation); all devices require iOS version 6.0 or later
- SharePoint 2013, SharePoint 2010, SharePoint 2010/2013 Online (Office 365) and SharePoint 2007

SharePoint Security & Privileges

By using SharePoint's web services to access SharePoint data, Colligo Briefcase respects all privileges defined on the site. Colligo Briefcase supports most standard sign-on processes supported by SharePoint, including support for default credentials and other specified credentials. Passwords are stored in the keychain.

Colligo Briefcase supports both Claims-based and Forms-based authentication. SharePoint by default does not provide web service permissions to anonymous users, so this permission level cannot be used for uploading documents to SharePoint.

For more detailed information on Briefcase security, please refer to http://www.colligo.com/media/document/The-Top-Five-Security-Challenges-Presented-by-Mobile-SharePoint-Access.pdf

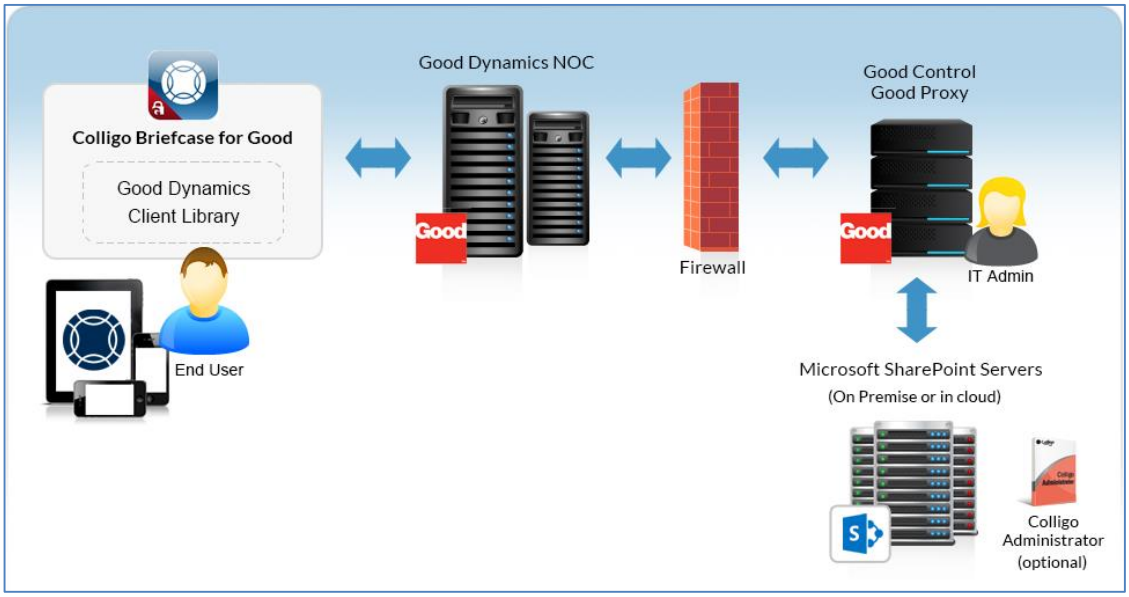
Colligo Briefcase for Good Technology

Good Dynamics enables secure connections between mobile clients and application servers that are behind the enterprise firewall. Colligo Briefcase for Good Technology has the following capabilities from an admin and user perspective:

- End-to-end encryption of data in transit between mobile clients and application servers
- Storing enterprise data on the device in a separate secure container, which can be remotely wiped by an admin without wiping the whole device
- Encryption with AES cypher technology (protects data at rest and data that's travelling between the client and the server)
- Enforce password policies
    - require user set passwords
    - set password policies around number and type of characters required and expiration of password
- Prevent data leakage (copy/paste from Briefcase to other applications is disabled and **Open In** functionality is locked down to other Good Dynamics applications)
- No need to use vpn to access corporate sites that would otherwise require it

The Good Dynamics infrastructure is composed of the following elements:

- **Good Dynamics Client Library**: the Client Library's API gives Good Dynamics access to user authentication, secure communications, secure storage and communication behind the firewall. The library also enforces security policies.
- **Good Dynamics Network Operation Center (NOC):** the NOC provides the secure communications infrastructure between the Client Library (on the device) and the Enterprise Servers (behind the firewall).
- **Good Dynamics Enterprise Servers**: There are two servers in the Good Dynamics infrastructure:
    - **Good Control Server**: this server manages the enterprise users, applications, and security policies
    - **Good Proxy Server**: this server provides the secure communications infrastructure between the NOC and application servers behind the firewall



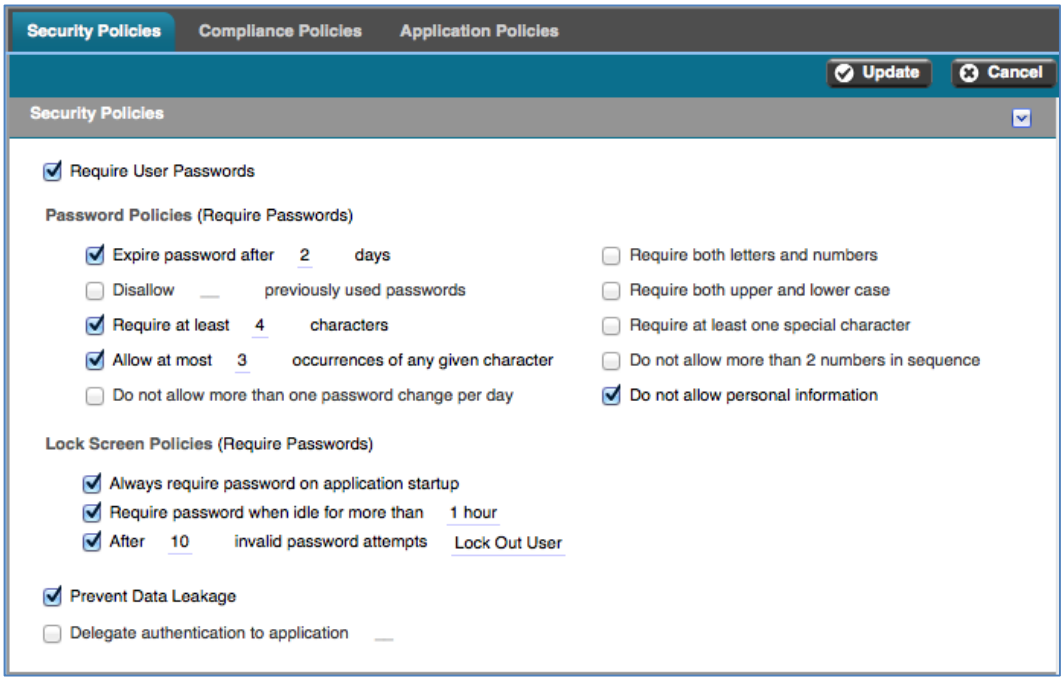
For more information about the Good Dynamics infrastructure, please see the Good Dynamics Admin and Developer Overview and the Good Dynamics Developer's Getting Started Guide at www.good.com.

In the Good Control policy management section, there are three Policy tabs that cover the options you can configure:

- Security Policies
- Compliance Policies
- Application Policies

Security Policies

You can use the following tab in Good Dynamics to configure the security policies in Colligo Briefcase:



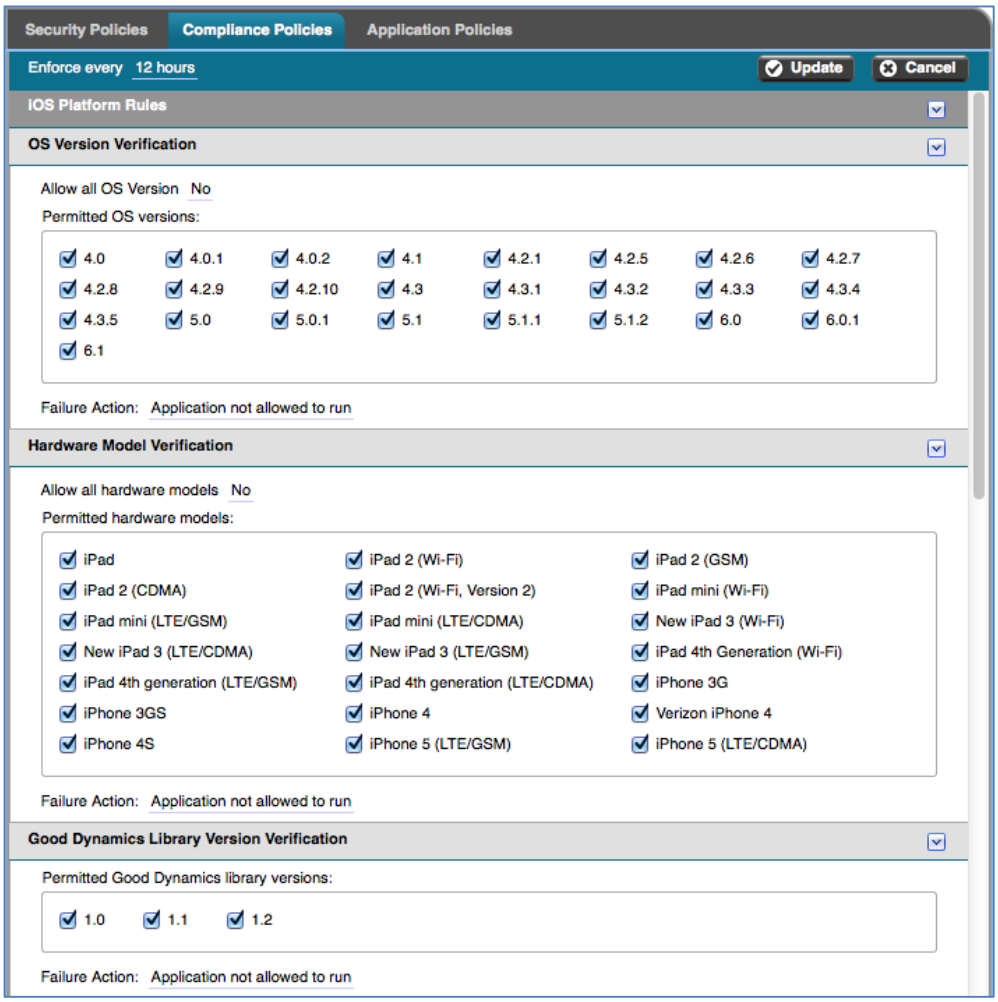
If **Require User Passwords** is checked, you can choose specific requirements for the **Password Policies** section to determine the type of password a user needs to enter, and also use the **Lock Screen Policies** section to set how frequently the password needs to be entered.

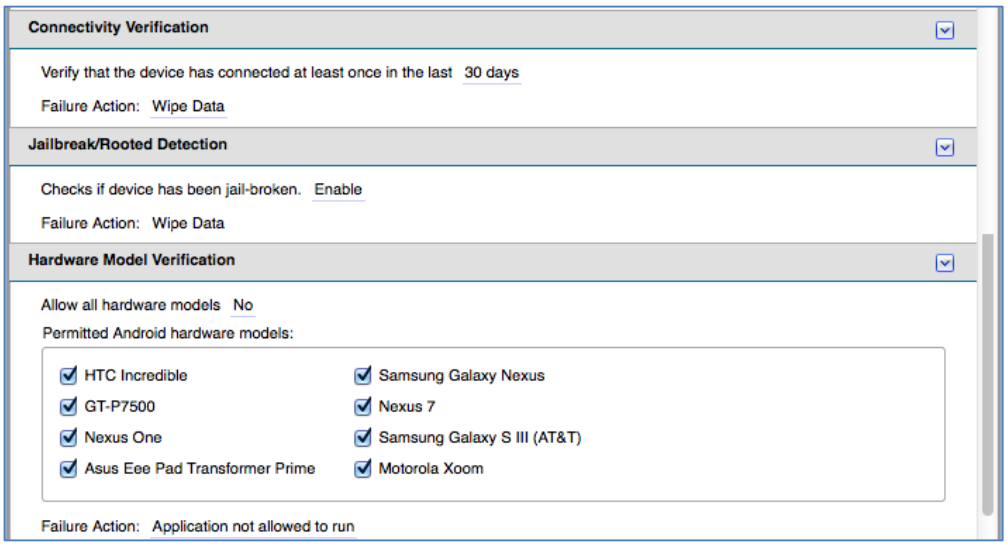
If the **Prevent Data Leakage** setting is enabled, the following restrictions are in place:

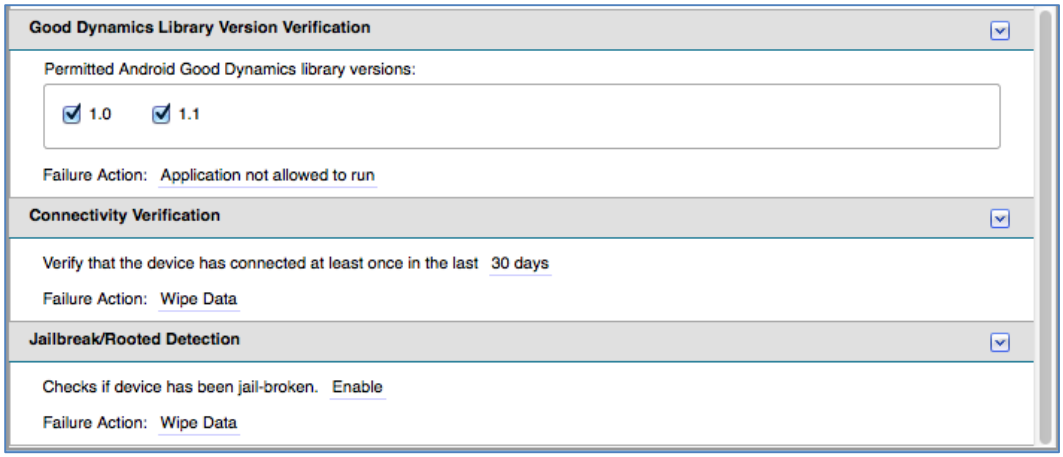
- **Cut/Copy/Paste**: users are prevented from copying data either into or out of the application
- **Open With/Open In**: users are prevented from opening documents with or in other native and/or third-party applications
- **Send/Save**: users are prevented from Sending or Saving data using native and/or third-party applications
- **URL-Based Invocation**: URL-based or other similar external interfaces that would allow the application to be launched are prevented

Compliance Polices

You can use the following tab in Good Dynamics to configure the compliance policies in Colligo Briefcase:

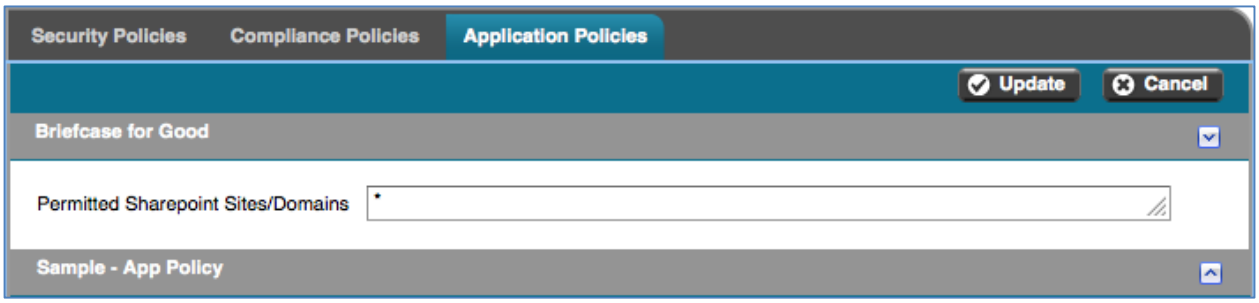






Application Policies

On the **Application Policies** tab, administrators can use the **Permitted SharePoint Sites/Domains** field to restrict which sites/domains can be used by a user or group of users.



To allow all sites to be added with no restrictions, enter *in the **Permitted SharePoint Sites/Domains** field.

To restrict the sites that can be added, create a whitelist of allowable sites in the **Permitted SharePoint Sites/Domains** field. This is a multi-line text field, so each site must be entered on its own line and may contain wildcards. For example:

- *.sharepoint.com
- sample.colligo.com/*
- companysite.ca

If a user tries to add a site in Briefcase that is not on this list, the following message displays:

Deploying Briefcase with Good Dynamics

The Briefcase with Good Dynamics app is available on the app store. To activate the app, administrators need to request access from Colligo in the Good Dynamics Network (GDN). To do this, complete the following steps:

1. Create an account on the GDN (http://be.good.com/community/gdn)
2. Go to the Good Dynamics Marketplace (https://begood.good.com/marketplace.jspa) and
3. Locate Colligo Briefcase in the catalog.
4. Click **Get Application** to request access to the app.
5. A Colligo representative will contact you to set up a trial, or to publish the app if the purchase is complete.
6. Briefcase then displays in your Good Control and you can provision keys for your users.

Custom Deployment

For customers wanting to use an MDM or have a custom deployment, complete the following steps:

1. Company purchases and deploys Good Dynamics.
2. Company purchases N Briefcase licenses from Colligo.
3. Colligo supplies an IPA file to Company. As with Briefcase Enterprise, this IPA file needs to be signed with the Company's Apple Enterprise Developer certificate.
4. Colligo enables the Briefcase license in Company's Good Dynamics console.
5. Company users download Briefcase via MDM or company's host.
   Briefcase is able to run within the Good Dynamics container on those devices due to the license being enabled in step 4.

Colligo Administrator

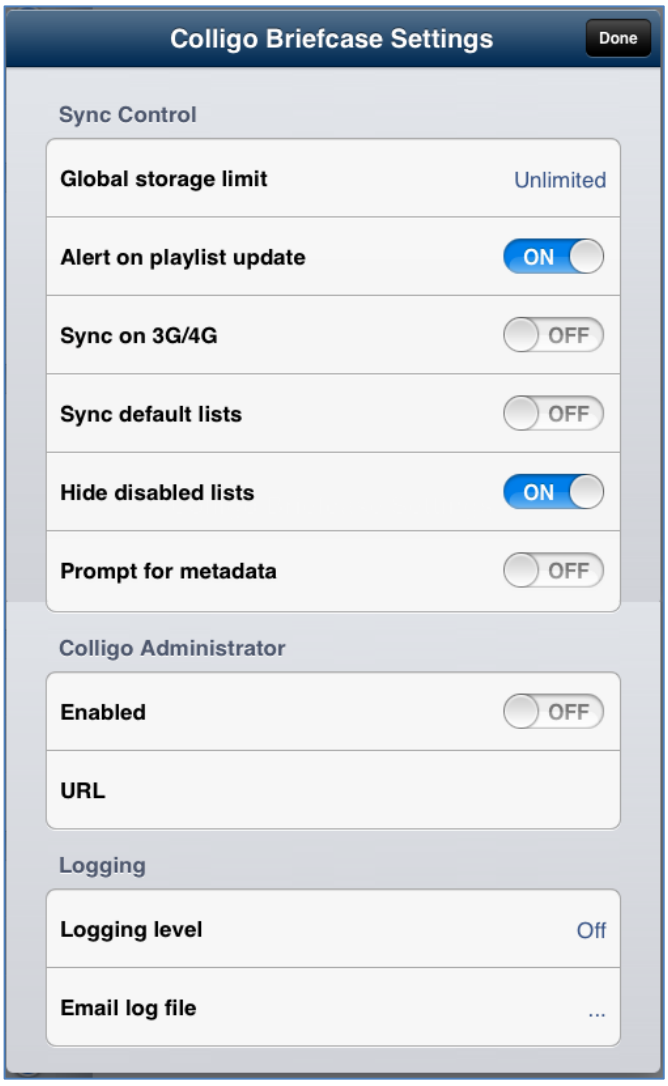
Colligo Administrator is a system for managing, configuring, and monitoring Colligo's SharePoint client products, including Colligo Briefcase, from a SharePoint server. Colligo Administrator consists of two components: the administration server, which is built on standard SharePoint (SharePoint 2010 or later) and the administration client, which is built into Colligo Briefcase and other client products.

Colligo Administrator allows you to centrally administer the sites that your users can access, as well as to set several security-based configuration settings. Colligo Administrator is only supported by Colligo Briefcase Enterprise and Colligo Briefcase for Good Technology (not Briefcase Pro or Lite). For more information, contact Colligo Sales.

Deploying the Administrator URL

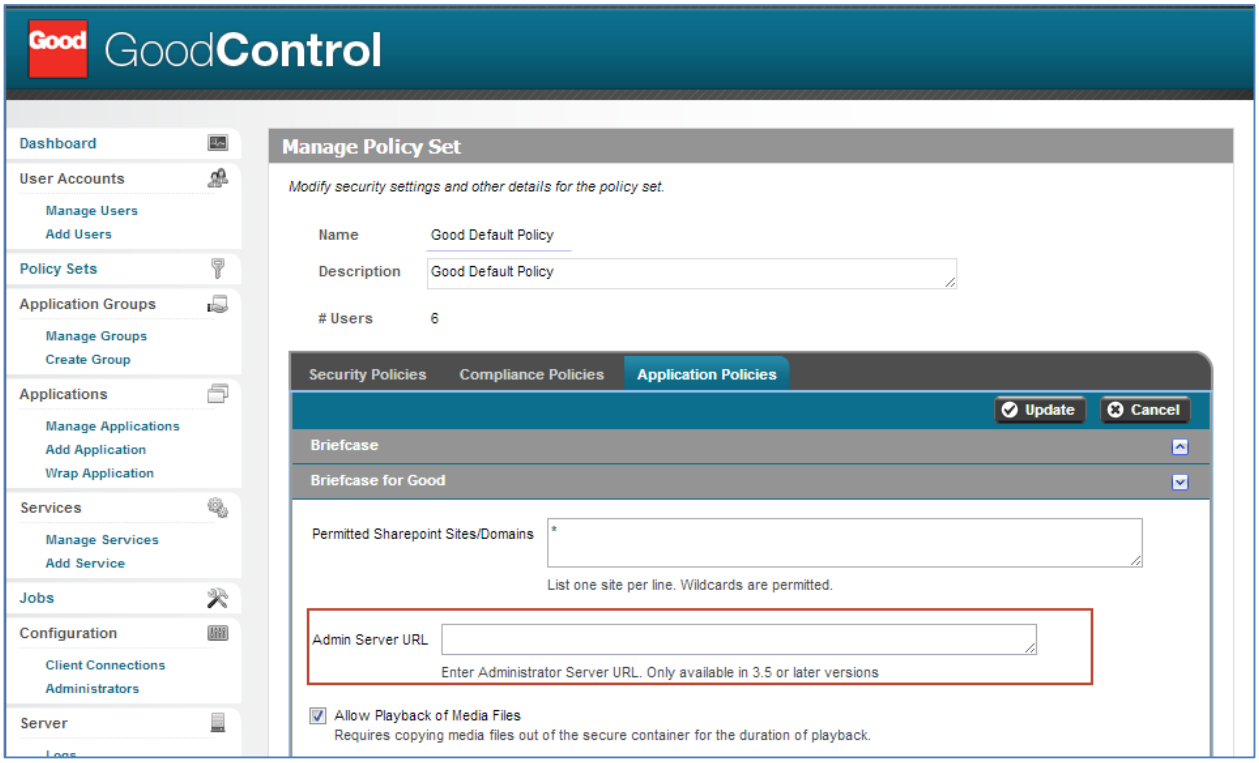
To use Colligo Administrator, complete the following steps:

1. Create the administrator site. For more information about creating the administration site and the Briefcase-specific options, see the **Colligo Administrator User Guide**.
2. In the **Colligo Briefcase Settings** dialog, in the **Colligo Administrator** section, turn the **Enabled** setting to **ON** and enter the URL into the **Server URL** field:



You can also use the Good Control server to push the Administrator URL out to your users. To do this, complete the following steps:

1. In the Good Control server, choose **Policy Sets**.
2. Select a policy and click the **Application Policies** tab.
3. Enter the Administrator URL in the **Admin Server URL** field:



4. Click **Update**.
   NOTE: once this setting has been pushed, the Colligo Administrator fields in the Briefcase app are disabled and users are not able to edit the URL field.

Configuring Settings using Colligo Administrator

You can configure the following settings for Briefcase using Colligo Administrator v1.3:

Configuration Title	Functionality	Possible Values
OpenIn Disabled	The option to open an item in a program is disabled when value is True	True / False
Email As Attachment Disabled	The option to email an item as an attachment is disabled when value is True	True / False
Email As Link Disabled	The option to email an item as a link is disabled when value is True	True / False
Print Disabled	The option to print a document is disabled when value is True	True / False
Default Sync Interval	Sets the default sync interval for sites	15, 20, 60, 1440 (one day)
Default Sync Limit	Sets the default sync limit for sites (in Mb)	0, 10, 20, 50, 100, 200, 500, 1000

Sync on 3G Default	Sets the **Sync on 3G/4G** setting to ON when value is True	True / False
OpenIn Approved Apps	The option to restrict the list of apps that display in the Open in list; any app listed in the Value field is an approved app and will display.	Any application name

For more information about Colligo Administrator, see
http://www.colligo.com/products/sharepoint/colligo-administrator/

Licensing

Colligo Briefcase for Good Dynamics is licensed on a per-user basis from Colligo Networks. Colligo will enable the purchased number of licenses in your Good Dynamics console.

Enterprise Deployment

Organizations can deploy the application either through their own enterprise app store within Good Technology, or by downloading the app from the iTunes App Store. Colligo can provide an IPA file for deployment through your enterprise app store.

Updates

New versions of Colligo Briefcase will be periodically released and be available for redeployment. Colligo will contact your company directly when a new version is available.

Enterprise Deployment

To upgrade to the latest version of Colligo Briefcase, you will receive a newly generated IPA file to integrate into your enterprise app store.

B2B with VPP

To upgrade to the latest version of Colligo Briefcase, a new IPA is uploaded to the Apple App Store. Users are notified of the update through the Apple App Store on their device, which can be installed directly.

Certificate Expiry

Certificate expiry applies only to Enterprise Deployments. Distribution Certificates last for one year, at which time they need to be re-generated. To renew the certificates, follow the process as described in the **Distribution Setup appendix.** Once the certificate has expired, no new installations or updates of the app can take place. However, existing installations will continue to function correctly. The updated certificate, identity, and provisioning must be provided to Colligo to create a new version of the App that can be distributed to you.

Obtaining your Distribution Certificate

To distribute your OS application, Apple requires your Team Agent to create a Distribution Certificate. Only your Team Agent can create this certificate and only that certificate enables application submission.

Generating a Certificate Signing Request

To request a Distribution Certificate, you first need to generate a Certificate Signing Request (CSR) utilizing the Keychain Access application in Mac OS X. The creation of a CSR prompts Keychain Access to simultaneously generate your public and private key pair, establishing your Distribution identity. Your private key is stored in the login Keychain by default and can be viewed in the Keychain Access application under **Keys**.

To generate a CSR:

1. In your **Applications** folder, open the **Utilities** folder and launch **Keychain Access**.
2. Choose **Keychain Access > Certificate Assistant > Request a Certificate from a Certificate Authority**.
   NOTE: If you have a private key highlighted (**Request a Certificate From a Certificate Authority with <Private Key>**) in the Keychain during this process, the resulting Certificate Request will not be accepted by the Provisioning Portal.
3. In the **User Email Address** field, enter your email address. Ensure that the email address entered matches the information that was submitted when you registered as a Developer.
4. In the **Common Name** field, enter Company_name.
5. Leave the CA Email Address blank. No CA Email Address is required.
6. Select the **Saved to Disk** radio button.
7. Click **Continue**.
8. Specify a file name and click **Save**.
9. Click **Continue**. The Certificate Assistant creates a CSR file on your desktop.

Submitting a Certificate Signing Request for Approval

Complete this procedure after generating a CSR.

1. Log in to the Provisioning Portal and navigate to **Certificates > Distribution.**
2. Click the **Add Certificate** button.
3. Click **Upload File** and browse to the CSR file.
4. Click **Submit**.
5. Approve your Distribution Certificate.

Downloading and Installing Distribution Certificates

1. In the **Certificates > Distribution** section of the Portal, control-click the **WWDR Intermediate Certificate** link and select **Saved Linked File to Downloads** to initiate download of the certificate.
2. After downloading, double-click the certificate to launch Keychain Access and install.
3. In the same area of the Provisioning Portal, click on the name of the Distribution Certificate to download.
4. On your local machine, double-click the downloaded .cer file to launch Keychain Access and install your certificate.

Saving your Private Key and Transferring to Other Systems

It is critical that you save your private key somewhere safe in the event that you need to build your application on multiple Macs or decide to reinstall your system OS. Without your private key, you cannot sign binaries in Xcode and will be unable to upload your application to the App Store or install your application on any Apple device. When a CSR is generated, the Keychain Access application creates a private key on your login keychain. This private key is tied to your user account and cannot be reproduced if lost due to an OS reinstall. If you plan to do development and testing on multiple systems, you need to import your private key onto all of the systems you'll be doing work on.

To export your private key and certificate for safe keeping:

1. Open the **Keychain Access Application** and select the **Certificates** category.
2. Highlight the certificate associated with your Distribution Certificate. Tap the arrow beside it to show the private key associated with it. Highlight both using Shift and select **File > Export Items**. Save your key in the Personal Information Exchange (.p12) file format.
   A prompt displays to create a password that will be used when you attempt to import this key on another computer.
3. Enter the password.
4. You can now transfer this .p12 file between systems. Double-click on the .p12 to install on a system. You will be prompted for the password you first entered above.

Creating and Downloading your Distribution Provisioning Profile for Distribution

To successfully build your application with Xcode for distribution via the App Store, you first need to create and download an App Store Distribution Provisioning Profile. These are different than the Development Provisioning Profiles that were used earlier in that Apple will only accept applications if they are built with an App Store Distribution Provisioning Profile.

NOTE: App Store provisioning profiles do not allow for a distribution built application to be installed on an Apple device.

To install your distribution ready application on a device, create an Ad Hoc provisioning profile:

1. Navigate to the **Provisioning** section of the **Provisioning Portal** and select the **Distribution** tab.
2. Select the **In House** radio button.
3. Enter the name for your Distribution Provisioning Profile.4. Confirm your Distribution Certificate has been created and is displayed.
4. Select your wild-card App ID to build all of your applications with your single Distribution Provisioning Profile.
5. Click **Submit**.
6. Click on the name of the Distribution Provisioning Profile to download the .**mobileprovision** file.
7. Drag the .mobileprovision onto the Xcode or iTunes icon in the dock to install.

Connecting InfoPath Form Lists and Libraries

Colligo Briefcase supports the viewing, editing, and creating of InfoPath forms in both lists and libraries. This feature is only available when users are online; however, InfoPath list items can be viewed when offline, and new items can be added by filling out the fields in list form, and the item is then uploaded on the next sync.

InfoPath Constraints and Supported Settings

InfoPath form types supported:

- InfoPath forms created for SharePoint Lists and SharePoint Form Libraries
- Web browser compatible forms

InfoPath Filler Forms, or any filler-specific controls, are not supported.
InfoPath rules (for field and button verification) and data connections are supported.
Additionally, Digital Signatures are currently untested.

Ribbon Commands

The following ribbon commands are supported:

- Submit
  NOTE: All submission options are supported, though only submitting to a SharePoint document library has been tested
- Save
- Save As
- Close
- Update

The following ribbon commands are not supported:

- Views
- Print Preview
  NOTE: These commands are actively hidden by Briefcase because they are not applicable to the iPad, iPhone, or iPod Touch

InfoPath Control Support

The following controls are supported for InfoPath Form Lists:

- Text Box
- Rich Text Box
- Drop-down List
- Check Box
- Option Button
- Date Picker
- Date/Time Picker
- List Box
- Person/Group Picker
- Button
- Calculated Value
- All containers
- Web browser compatible custom controls are also supported

The following controls are not supported for InfoPath Form Lists:

- File or picture attachments.
- Users can manually attach files/pictures/sketches to InfoPath Form List items through Briefcase.

The following controls are supported for InfoPath Form Libraries:

- Text Box
- Rich Text Box
- Drop-down List
- Combo Box
- Check Box
- Option Button
- Date Picker
- Date/Time Picker
- Multiple-Selection List Box
- List Box
- Bulleted List
- Numbered List
- Plain List
- Person/Group Picker
- Button
- Calculated Value
- All containers
- Hyperlink
- Picture
- Web browser compatible custom controls are also supported

The following controls are not supported for InfoPath Form Libraries:

- Picture Button
- Ink Pad/Signature
- File Attachment

Viewing InfoPath forms

All saved/submitted InfoPath forms (xml) are viewable as forms outside form libraries as long as the corresponding .xsn files are accessible to Briefcase. For example: If a form in library A is filled out and submitted to library B, users who access the submitted .xml file in Library B should have no issues viewing that .xml file as an InfoPath form, as long as the .xsn associated with that form is accessible to the user.