BlackBerry Work, BlackBerry Tasks, and BlackBerry Notes Administration Guide for Good Control

©2018 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. All other trademarks are the property of their respective owners. This documentation is provided "as is" and without condition, endorsement, guarantee, representation or warranty, or liability of any kind by BlackBerry Limited and its affiliated companies, all of which are expressly disclaimed to the maximum extent permitted by applicable law in your jurisdiction.

Table of Contents

Introduction 7

Environment and System Prerequisites 8

Required BlackBerry Dynamics Versions 8

Supported Exchange Versions 8

Configuring the BlackBerry Work App in Good Control 9

Configuring Client Connections 10

Required BlackBerry Work Connections to Good Proxy 10

Adding Client Connections 10

Configuring Exchange ActiveSync (EAS) 11

Whitelisting Your EAS Server(s) 11

Adding the JSON Configuration for Autodiscover, EAS, EWS Connectivity 12

Adding Applications and Users in Good Control 15

Setting BlackBerry Work Application Policies 16

Setting BlackBerry Work Security Policies 22

Application passwords 22

Fingerprint policies 23

Authentication Delegation 23

Prioritizing Delegation 23

Assigning Authentication Delegates 24

Overriding Short Setup 24

Disabling EWS Features 24

Setting Up Support for Creating and Joining a Skype for Business Meeting 25

Troubleshooting 27

Enabling Exchange ActiveSync (EAS) 27

Configuring Exchange Autodiscover 28

Implementing KCD for BlackBerry Work 28

Environments Supported 29
Additional Requirements 29
Limitations 29
Preparing Your Environment for KCD 30
Creating the IIS Alternate Service Account 31
Configuring Delegation to Good Control 33
Configuring the BlackBerry Work App for KCD 34
Setting Up S/MIME 34
Device Verification and Testing 35
Device Provisioning and Activation 35
Appendix A – Content Synchronization and Notifications on iOS 37
Foreground Operation 37
Background Processing 37
Badge Count Updates 38
VIP Notifications 39
Scenarios and Behaviors 40
Troubleshooting 40
Troubleshooting Initial Setup 40
Troubleshooting Foreground Operations 41
Troubleshooting Background Processing 41
Deploying the BlackBerry Work Client 42
Phase I: Environment Readiness 42
Phase II: Easy Activation 43
Initial Setup 43
Appendix B – BlackBerry Work for Android Wear 44
Appendix C – GC Server Configuration Settings and Definitions 46
Common Guidelines 46
Definitions 48
Value Types 48

Security Settings 48
BEMS Settings 49
Exchange Settings 49
Client Settings 51
Other Settings 51
Appendix D – GFE to BlackBerry Work Deployment and Migration 52
GFE Material Parity 52
BEMS-BlackBerry Work/GFE Feature Disparity 52
Appendix E – File Types Supported by BlackBerry Work 53
Appendix F – Exchange Active Sync (EAS) Search Limits 55
ActiveSync Search Command 55
Compose Email Recipient Search 55
Appendix G – Whitelisting Native and Third-Party Apps for "Open In" 56
Appendix H – Changing Mail Message/Attachment Limits in Exchange 59
Configuring Max Message Size 59
Configuring Attachment Size Limit 59
Resolving EAS Max Request Length Exceeded Errors 60
Appendix I – BlackBerry Work Badge Count 62
New Mail 62
Unread Mail 62
Optimization and Limitations 62
Administration Policy 63
Appendix J – BlackBerry Tasks and BlackBerry Notes 64
Introduction 64
Setup 64
Setting BlackBerry Tasks and Notes Application Policies 64
Notification Policy (Tasks Only) 65
Configuration Settings 65

Exchange Settings 65
App Settings 67
Appendix K – Exchange Classifications and Caveats 68
Appendix L – Using ADAL for Authentication 71
Setting up GC 71
Obtaining an Azure App ID 71
Related Links 72
Microsoft Exchange Server Deployment Assistant 72
Hybrid Deployment Prerequisites 72
Hybrid Configuration Wizard 72
MS Video 72
"Office 365 Exchange Hybrid Deployments Busting The Autodiscover Myth" 72
Exchange Q & A: Handling Hybrid Environments 72
"Do I really need to use ADFS in O365 / Azure AD?"l 72
Plan Your ADFS Deployment 72
Office 365 SSO: A Simplified Installation Guide 73
Hybrid Identity Required Ports and Protocols 73
Connectivity Prerequisites 73

Determining whether you should upgrade to BlackBerry UEM

If you require MDM or MAM capabilities, you must manage BlackBerry Dynamics apps using BlackBerry UEM. When you upgrade from Good Control to BlackBerry UEM, you not only get to use the great feature set that Good Control provides but you also get to take advantage of an enhanced feature set such as:

- Support for more policies for operating systems
- Better app management
- More container types
- Improved administration and provisioning
- Advanced connectivity and networking
- Expanded compliance and integrity checking
- Additional email, content, location, and certificate features
- Access to BlackBerry Web Services APIs

For more information on the benefits of using BlackBerry UEM, see Benefits of upgrading from Good Control to BlackBerry UEM.

System requirements

To use BlackBerry Work, your organization must meet the following requirements:

Item	Requirement
Management solution	Good Control version 2.3 or later, Good Proxy version 2.3 or later
Device OS	For device OS compatibility, see the Mobile/Desktop OS and Enterprise Applications Compatibility Matrix.

- **Cloud-based BEMS On-premises Exchange**
  a. You must expose EWS and Autodiscover from your on-premises Exchange to the Internet on port 443.
  b. Both Basic Authentication and Windows Authentication are supported for EWS and Autodiscover.
- **On-premises BEMS Cloud-based Exchange**
  a. You must expose EWS and Autodiscover from Cloud-based Exchange to On-premises BEMS on port 443.
  b. Although both Basic Authentication and Windows Authentication are supported by BEMS, be advised that certain cloud vendors—for instance, O365 and Rackspace—only support Basic Authentication. Please check with your specific cloud vendor for details.
- **On-premises BEMS On-premises and Cloud-based Exchange** (i.e., Hybrid Exchange setup)

a. You must expose EWS and Autodiscover from Cloud-based Exchange to On-premises BEMS on port 443.
b. Although both Basic Authentication and Windows Authentication are supported by BEMS, be advised that certain cloud vendors—for instance, O365 and Rackspace—only support Basic Authentication. Please check with your specific cloud vendor for details.
c. A BlackBerry Admin mailbox must first be created on premise and then migrated to the cloud
d. The BlackBerry Admin account must have Impersonation rights on both the On-premises and O365 Exchange systems. For details, see KB2725.

For additional information on configuring EWS and Autodiscover for external access, refer to the pertinent Microsoft articles on TechNet:

- Configuring the Autodiscover Service for Internet Access
- Configuring EWS for External Access

Configuring the BlackBerry Work App in Good Control

Before you can configure an application like BlackBerry Work in Good Control it must be registered.

For complete instructions on adding BlackBerry Work and BlackBerry Presence in Good Control, see **Registering a New Application** in your Good Control online help utility.

Once the app is registered, you can configure application use privileges and permissions, using the following instructions in conjunction with your Good Control OLH.

A few basic configuration settings are necessary so that Good Control can properly support BlackBerry Work application users. These include:

- Configuring Client Connections
- Configuring EAS for the BlackBerry Work app
- Adding Applications and Users
- Device Provisioning and Activation

Note: The BlackBerry Work application must be published in Good Control. For prerequisite details on setting up Good Control, see *Good Control and Good Proxy Installation Guide*. To learn how to add the application in Good Control, see "Registering a New Application" in the GC console's online help.

Configuring Client Connections

Good Proxy (GP) maintains the secure connection between your enterprise and the Good NOC. A GP connection is used for secure communication relay, as well as presentation of the GD Push Channel service to BEMS and other enterprise application servers.

Because GP is installed behind the enterprise firewall and establishes a secure outbound connection to the NOC, there is no need to open an inbound port in the firewall and no need to use a VPN.

Clustering GPs adds relay capacity in addition to providing HA/DR.

Required BlackBerry Work Connections to Good Proxy

The total number of Good Proxy connections required by BlackBerry Work depends on the features and services being

used in BlackBerry Work. The following table breaks out the various features and the respective number of Good Proxy connections required.

BlackBerry Work Feature/Service	# of GP Connections
Exchange ActiveSync	1
Exchange Web Services	1
Push Notifications	1
Presence	1
Docs	2
Miscellaneous	1
Total	7

Although, theoretically, the maximum number of connections is 7, all 7 connections are unlikely to be used all at once. For example, Docs connections are only used when a user is using Docs within BlackBerry Work. Realistically, the average connection usage is between 3 and 5.

Nonetheless, both the average and maximum number of connections must be considered in determining the number of GP servers you will need to deploy to accommodate your mobile user community.

Adding Client Connections

From the Good Control console navigator, click **Connectivity Profiles** under **POLICIES**, then click **Master Connection Profile**.

Next, with the **Infrastructure** tab open, locate (scroll down to) the **Additional Servers** section. This is a list of specific servers with which all GD applications can connect. Add servers to this list instead of using the **Allowed Domains** list if you want to restrict access so that GD applications can only connect to certain servers—like BEMS and Exchange—and not to every machine in a domain.

> **Note:** Here, it's important to add an entry for the Exchange ActiveSync server on port 443.

To add a new allowed server:

1. Click **EDIT**, then scroll down to the bottom of the list and click **ADD**.
2. Enter the server's fully qualified **Host Name**.
3. Enter **8443** as the **Port**.
4. Configure a primary and secondary GP cluster for the server, if applicable. Connections through GP servers in the primary cluster are attempted first, and if no responses are received, connections are attempted through GP servers in the secondary cluster.
5. Click **Add**, then click **Save**.

To remove a server from the list:

1. Click the corresponding ⊗ for the server you wish to delete.
2. Click **Save**.

Configuring Exchange ActiveSync (EAS)

Before the BlackBerry Work app can be configured to use PNS, it must first be configured for EAS. This will allow your

users to easily enroll in EAS when they activate their BlackBerry Work app. This is accomplished from your Good Control console.

There are several parts to this procedure:

- Whitelisting the EAS server(s) in Good Control
- Adding the correct JSON configuration for EAS

Instructions for each part are listed in order below.

Whitelisting Your EAS Server(s)

A whitelist is a list or register of servers and/or applications that are being provided a particular privilege, service, mobility, access or recognition. Those on the list will be accepted, approved or recognized. In other words, whitelisting is the opposite of blacklisting—the practice of identifying servers and applications that are denied, unrecognized, or ostracized.

To whitelist your EAS server(s) in Good Control:

1. In the navigator (left-hand panel) under **POLICIES**, click **Connectivity Profiles**, scroll down to **Additional Servers**, and click **EDIT**.
2. Scroll down to the bottom of the server list and click **ADD**.

1. Enter the server's fully qualified **Host Name**.
2. Enter **443** as the **Port**.
3. Configure a primary and secondary GP cluster for the server, if applicable. Connections through GP servers in the primary cluster are attempted first, and if no responses are received, connections are attempted through GP servers in the secondary cluster.
4. Click **Add**.
5. Add more EAS or Autodiscover servers as appropriate, then click **Save**.

Adding the JSON Configuration for Autodiscover, EAS, EWS Connectivity

BlackBerry Work iOS and Android clients are designed to synchronize content from a MS Exchange server using the Exchange Active Sync (EAS) protocol. Additionally, the clients rely on the Enterprise Exchange Web Services (EWS) protocol to support calendar capabilities (event forwarding and attachment retrieval). The clients require a reliable mechanism by which they may determine the appropriate server endpoints to which they can make their EAS/EWS requests.

In BlackBerry Work client releases prior to v2.2, the device clients have used a combination of Application Configuration JSON, naming conventions and client side autodiscovery to locate the server endpoint. In cases where the client is unable to determine the proper endpoint the user is presented with 'the long form' into which the informed user can specify the initial server endpoint.

For BlackBerry Work clients v2.2 and later, the GEMS Server provides server-side autodisocver services for EAS and EWS.

JSON (JavaScript Object Notation) is a lightweight data-interchange format that's easy for humans to read and write, and, for BlackBerry Work and its supporting infrastructure, accurately parse and generate. JSON is based on a subset of the JavaScript Programming Language, Standard ECMA-262 3rd Edition.

JSON is built on two structures:

- A collection of name/value pairs. In various languages, this is realized as an object, record, struct, dictionary, hash table, keyed list, or associative array.
- An ordered list of values. In most languages, this is realized as an array, vector, list, or sequence.

With the autodiscover feature, the client checks for the EWSServerURL and EASServer specified in the configuration file and uses these endpoints to connect/sync. If this server is not specified or available, the GEMS autodiscover feature (available in version 2.2 and above) is used. If unavailable, the Autodiscover URL specified in the configuration file is used to perform automated discovery and the discovered EAS URL is used to connect/sync; if not set, the EWS URL is derived from the discovered EAS URL.

To add the correct JSON configuration to Good Control:

1. Under APPS, click Manage Apps, serch for or scroll down to BlackBerry Work and click it.
2. Click the BlackBerry Dynamics tab and then in the Server section click Edit.
3. In the **Configuration** field, define the following by copy/pasting or manually entering a configuration as shown in the example below:

   "EASServer":"*EAS server fully qualified DNS name*"

   "EWSServerURL":"*https://dev.mycompany.net/EWS/Exchange.asmx*"

   or

   "UseServerAutodiscover":"true"

   "AutodiscoverURL":"*<https://autodiscover.mydomain.com/autodiscover/autodiscover.xml>*"

   You should specify one or the other of these settings. Specifying a EASServer and EWSServerURL will bypass the Autodiscover steps. If you have GEMS 2.2 and above,GEMS is able to assist Autodiscover more efficiently. This can be turned on using UseServerAutodiscover config.

   Optional:

   "EASAuthenticationMethods":["Negotiate","NTLM","Basic"]

   "EWSAuthenticationMethods":["Negotiate","NTLM","Basic"]

   "AutodiscoverTimeout":60

   These configurations can be used to fine tune the Autodiscover and EAS/EWS Connection negotiation for your network configuration. More detail on the configs in provided in – GC Server Configuration Settings and Definitions .

   Example:

```
{
   "serverListReshufflePeriodInMinutes":30,
   "serverListQuarentinePeriodInMinutes":5,
   "disableSSLCertificateChecking":"true",
   "skipShortSetup":"false",
"mycompany.com":{
   "EASDomain":"g3",
   "EASServer":"ex2010.mycompany.com",
   "EWSServerURL":"https://dev.mycompany.net/EWS/Exchange.asmx"
   "useKCD":"false",
   "skipShortSetup":"true"
},
   "dev.mycompany.net":{
      "AutodiscoverURL":"https://dev.mycompany.net/autodiscover.xml",
```

```
    }
}
```

Before copying and pasting the configuration into Good Control, use **JSONLint** (http://jsonlint.com/) to validate the syntax of your configuration. **JSONLint** will check and make sure the formatting is correct.

If you don't receive a "Valid JSON" response, then it means there is a formatting issue with the configuration. Please correct it before copying it to Good Control. See Appendix B for the complete list of BlackBerry Work server configuration settings and their definitions.

> **Important:** The value of **"***<email domain for end users>***"** must match the email suffix of your users in Good Control or the BlackBerry Work client will not be able to retrieve the predefined EAS configuration from Good Control.

If you support multiple email suffixes, add an additional "domain block" configuration in the JSON; for instance:

```
{
  "disableSSLCertificateChecking":"true",
  "domain1.com": {
     "EASDomain":"domain1",
     "EASServer":"eas1.domain1.com",
     "EWSServerURL":"https://dev.mycompany.net/EWS/Exchange.asmx"
  },
  "domain2.com": {
     "EASDomain":"domain2",
     "AutodiscoverURL":"https://autodiscover.domain2.com/autodiscover/autodiscover.xml",
  }
}
```

Initially, you should add the BlackBerry Work app to the **Everyone** Application Group.

It is also highly recommended at this point in the configuration process that you test and verify EAS communications and functionality. This is best done by provisioning a client device with the BlackBerry Work app and giving it a road test.

Adding BEMS to the BlackBerry Application Server List

The BlackBerry Work client checks the BlackBerry Work server list for available BEMS instances hosting the Presence service. Hence, the list must be populated with at least one BEMS machine configured for the BlackBerry Enterprise Services entitlement app.

When multiple BEMS hosts are listed, you can use BlackBerry 's **Preferred Presence Server Configuration** parameter to set up a presence affinity association (see Configuring Presence Affinity for BlackBerry Work).

To add BEMS to the BlackBerry Work application server list:

1. Under **APPS**, click **Manage Apps**, search for or scroll down to **BlackBerry Work** and click it.
2. Click the **BLACKBERRY DYNAMICS** tab, then, in the **Server** section, click **EDIT**.
3. Enter the BEMS host FQDN in the **Host Name** field, then enter **8443** under **Port**.

> **Note**: Unless you import a publicly verifiable certificate into the BEMS Java keystore, please be aware of the following:
>
> 1. Access to the BEMS Dashboard from a browser will show an untrusted SSL certificate.
> 2. You will need to upload the BEMS certificate to Good Control.

4. If you have additional BEMS hosts, configure them for the application in the same way, after clicking to add a new row.
5. Click **Save** to commit your changes.

Configuring Presence Affinity for BlackBerry Work

Presence affinity for BlackBerry Work is configured in Good Control's **Application Policies**. Presence affinity is optional. Be aware, however, that once you set affinity, it takes precedence.

> **Caution:** When a distributed computer system is truly load balanced, each request is routed to a different server. This load balancing approach is diminished when server affinity techniques are applied.

To set Presence Affinity for BlackBerry Work:

1. In the Good Control navigator under **POLICIES**, click **Policy Sets**.
2. Locate the policy you want to apply and click it.
3. Click the **APPS** tab, then expand **APP SPECIFIC POLICIES**.
4. Scroll down to **BLACKBERRY WORK** and click it. The **App Settings** tab should be open by default. If not, click it.
5. Scroll to **PREFERRED PRESENCE SERVER CONFIGURATION**.
6. In the **Server Hosts** field, enter in the FQDN of your BEMS host and a colon followed by port **8443**. As desired, add more servers separated by a comma and no space.
7. Click **Update**.

Repeat for every other policy that will govern BlackBerry Work Presence.

Configuring Docs Server Affinity for BlackBerry Work

> **Caution:** As pointed out for the Presence service, when a distributed computer system is truly load balanced, each request is routed to a different server. This load balancing approach is diminished when server affinity techniques are applied. Be aware that once you set affinity, it takes precedence.

To set server affinity for Docs in BlackBerry Work:

1. Follow the first four steps under Configuring Presence Server Affinity for BlackBerry Work.
2. Scroll down to **PREFERRED DOCS SERVER CONFIGURATION**.
3. In the **Server Hosts** field, enter in the FQDN of your BEMS host and a colon followed by port **8443**. As desired, add more servers separated by a comma and no space.
4. Click **Update**.

Repeat for every policy that will govern BlackBerry Work Docs.

Adding Applications and Users in Good Control

By default, every user is assigned the “Everyone” group. If you plan to use the default, simply add the BlackBerry Work app to the **Everyone** Application Group.

Refer to your Good Control online help utility for complete instructions on adding applications like BlackBerry Work, BlackBerry Notes,Creating the IIS Alternate Service Account and BlackBerry Tasks, as well as new user accounts, and then modifying policies and permissions.

Setting BlackBerry Work Application Policies

Policy sets contain rules that govern the security of GD applications and rules specific to the devices and OS versions configured in Good Control.

To set an application-specific policy for BlackBerry Work:

1. In the Good Control console navigator (left-hand panel) click **Policy Sets**, select a policy to clone and/or modify by clicking it, then click the **APPS** tab and expand the **APP SPECIFIC POLICIES** list.
2. Scroll down to select **BLACKBERRY WORK** from the list by clicking it. The **App Settings** tab opens by default.

   Check the "Enable automated autodiscover" checkbox.

   As you scroll down, there are a number of options you may wish to consider, namely:

   a. **AUTHORIZED EMAIL DOMAINS** – sets authorized email domains; used to display a warning to users who are attempting to share information outside of a trusted domain.
   b. **EXTERNAL EMAIL MARKING** - To add warning text to subject line when sending to external domains, check the box to enable "Prepend tag on subject on external emails." Then add custom text that will be prepended to the sender's subject line when sending to external domains. There is no limit to the number of characters in the text.
   c. **AVATAR PHOTOS** – enables display of sender/contact photographs. Disabling avatar photos will show the user initials instead of photo.
   d. **ENABLE SEARCHING EMAILS ON SERVER** - Allows users to search emails on the server. Deault is ON.
   e. **DIAGNOSTICS** - Allows users to perform app diagnostics on their device. Default is ON.
   f. **BLACKBERRY GATEKEEPING SERVICE** - Enables use of the BlackBerry Gatekeeping Service. Default is OFF. For more on this service, refer to using-gatekeeping.html.

2. Click the **Notifications** tab to select/deselect the application features you want to enable for your users.

Scroll down to reveal additional settings. These include:

- **SELECT LEVEL OF DETAIL IN EMAIL NOTIFICATIONS**
  - No notification
  - No details in notification
  - Sender only
  - Sender and Subject
  - Sender, Subject and Preview (Android only)
- **SELECT LEVEL OF DETAIL IN CALENDAR NOTIFICATIONS**
  - No notification
  - No details in notification
  - Meeting Time only
  - Meeting Time and Subject
  - Meeting Time, Subject, Location and Preview (Android only)

- Show only generic notifications when app is locked (Android only). If the app UI is timed out, only generic information is displayed in notifications. Notification policy settings are respected once user has logged back into the app.
- Show notifications on connected wearable devices (Android Wear only). Notification policy settings are respected for determining the notification content on Android Wear devices.
- **ADDITIONAL OPTIONS FOR NOTIFICATIONS ON ANDROID WEAR DEVICES**
  - Notification for VIP Contacts
  - Notification for anyone
  - Notification with voice reply for anyone
- **IOS APP ICON BADGE** - Allow user to choose between “Unread Mails” and "New Mails" as their default Badge count on the App Icon.If disabled, the App Icon Badge will reflect the number of new emails received since last closing the app. The user will not see an option in Settings to select “Unread Mails” as an App Icon Badge count preference.

3. Click the **Address Book** tab and set your user permissions according to your IT policy for synchronizing contacts. Scroll down to reveal additional settings. Again, you can always change these settings later, which include:
   a. **ADDRESS BOOK SYNC** - allow/disallow synchronizing of BlackBerry contacts on the device, with selective access to the fields you choose to enable; set the max length for the notes field; and allow/disallow contact synchronization even if iCloud is enabled.
   b. **CALLER ID**: Select the Allow device to use BlackBerry Contacts option if you want to allow BlackBerry Work to access the user's BlackBerry Work contact list to display contact name for incoming and outgoing phone calls.
   c. **GAL SEARCH** – sets the max number of results to display when searching the global address list (GAL).
   d. **RECIPIENTS** (Enable caching) - Policy control for recipient suggestions cache. The recipient cache is populated from Sent Messages and Contacts. The cache is used to offer autocomplete of the recipients during email composition. Default is Enabled.

4. Click the **Interoperability** tab, then set your:
   a. **CAMERA AND DEVICE PHOTO GALLERY PERMISSIONS** – allowing access to either the device camera or photo gallery, or both
   b. **VOICE** options – to allow users to tap a phone number to dial using the device's native phone and/or an entitled and installed GD VOIP application
   c. **SMS** options – to allow users to initiate their native SMS app by tapping the SMS icon and/or to use entitled and installed GD SMS apps
   d. **MISC** options – to allow access to the user's native browser and/or native map application
   e. **RSA SECUREID APP** – to enable two-factor authentication integration with a third-party RSA SecureID app using a CTF token seed

      Note: BlackBerry Work supports CTF-based and file-based provisioning using BlackBerry Access, as well as CTF-based provisioning using a native RSA SecureID application. For additional guidance on configuring RSA soft-token authentication and provisioning the token seed record your organization sends to users, see the *BlackBerry Access Administration Guide*. Bear in mind that changes in secure token format may require consultation with BlackBerry 's RSA Infrastucture team.

   f. **FILE HANDLING** permissions – allowing/blocking the transfer of files to third-party native apps on the user's device. Here, you can selectively whitelist/blacklist specific apps by app ID (Example:

"**ABCDE12345.com.company.appname # *platformID***". A valid platformID is either iOS or android. No hashtag and platformID indicates file transfer privileges are allowed across all platforms.

g. Skype for Business

a. Allow creation of Skype For Business meetings in Calendar - This feature adds an addition option in the Calendar window for meeting creation, to create Skype For Business meetings.

b. Allow launching Skype For Business meetings on the mobile device. - This feature allows launch of Skype For Business on the device, to join meetings and, from a Contact's page, to make voice and video calls. (Video calls, Android only)

c. Domain of Skype For Business meeting link - Enter the fully qualified domain name for Skype For Business meeting links, to allow internal users to tap "Join meeting" in the event details window.

Refer to Setting Up Support for Creating and Joining a Skype for Business Meeting for information on setting up Skype For Business.

See Appendix G for a Voltage SecureMail example of whitelisting a third-party application for file export.

5. Click the **Docs and Attachments** tab to set your policy governing:

a. **DOCS REPOSITORY** – enable/disable a file repository on the device, enabled/disable local and/or server docs repositories, and force users to save pending uploads.

> **Note:** By default users are alerted about any pending uploads every 24 hours. With Forced Pending Uploads Policy enabled, users are blocked from taking any document related actions in BlackBerry Work until all files are successfully uploaded to the server.

The Server Docs Repository setting applies to members of a Docs service-entitled App Group only. To entitle Docs Services, see "Entitling Users" under "Configuring Good Control for the Docs Service" in the *BEMS Installation and Configuration Guide.*

b. **SENDING ATTACHMENTS** – block or permit outgoing attachments by specifying a maximum size and the file extensions allowed or disallowed.

c. **RECEIVING / OPENING ATTACHMENTS** – block or permit incoming attachments by specifying a maximum size and the file extensions allowed or disallowed.

d. ENABLING BOX AS AN ENTERPRISE REPOSITORY - allow users to utilize Box as an enterprise docs repository within the Docs module. Default is "Off."

6. Click the **Classification** tab to enable email classification and caveat markings, such as **INTERNAL**, **CONFIDENTIAL**, **NO FORWARD**, and/or **NO REPLY**. Edit the XML classes onscreen according to the classificatons

and caveats you wish to make available to users in this policy. For an example file, refer to – Exchange Classifications and Caveats .

7. Click the **Basic Configuration** tab to configure the following settings. Note that these settings are also available using the application config JSON. In order for the GC settings to take effect, the app settings JSON must be empty.

   a. **SECURITY SETTINGS**

      Disable SSL Certificate Checking - Disables SSL certificate verification for ActiveSync / Exchange Web Services in test and POC environments.

      Expect Kerberos Constrained Delegation and supress username/password entry for Exchange - If enabled, Kerberos Constrained Delegation will be used for logging into Exchange, otherwise NTLM / Basic authentication will be used.

      Clients must have individual login certificates (SSL) uploaded in the GC - If enabled, clients must have individual login certificates (SSL) uploaded in BlackBerry Control Console. These certificates will be used for login in place of basic credentials (login / password).

   b. **ENTERPRISE SERVER SETTINGS**

      Server List Reshuffle Period (minutes) - Frequency that server list (if present) will be reshuffled, for load balancing purposes.

      Server List Quarantine Period (minutes) - If a BlackBerry Enterprise Server is not working, BlackBerry Work will wait this period before retrying.

   c. **CLIENT SETTINGS**

      Sync Email Body Size (Kb) - Size in Kbytes of the partial message body downloaded from server if the user selects the option to download partial message content.

      Use BEMS to perform AutoDiscover of the EAS/EWS endpoint for the user - When set to "true," client will use the BlackBerry Server Autodiscover service to determine the EAS/EWS endpoint for the user.

      Create and consume rights-managed email messages - Exchange Information Rights Managements for mail. IRM needs to be enabled for user mailboxes on Exchange as a pre-requisite.

   d. **OTHER SETTINGS**

      Send Feedback Email Address

      Sends client feedback email to "bbwadmin@acme.com" as an example. Add multiple comma delimited recipients as needed.

      Report Phishing Email Address - nables users to report emails considered as phishing. The reported emails are being forwarded to the email address provided in this field then moved to Trash folder.

   e. **ACCOUNT SETUP**

      Skip Email Short Form Setup - When true, takes the user directly to the long setup form, requiring user input of a recognized AD username, password, and domain during device activation.

f. **ACTIVESYNC AND AUTO DISCOVER AUTHENTICATION METHODS (IOS ONLY)**

Use following Authentication Methods:

- Negotiate
- NTLM
- Basic

Select allowed authentication method from Exchange Active Sync and Autodiscover setting. If only certain authentication methods are supported from Exchange, set those values to minimize the user setup time. (E.g. if Auto Discover and ActiveSync IIS Auth Settings are set to allow only NTLM and Basic, then de-select Negotiate in above app setting.) If none are selected above, default Exchange setting will be used. Do not check any of these options if using client-based authentication.

g. **EXCHANGE WEB SERVICES AUTHENTICATION METHODS (IOS ONLY)**

Use following Authentication Methods:

- Negotiate
- NTLM
- Basic

Select allowed authentication method from Exchange Web Services setting. If only certain authentication methods are supported from Exchange, set those values to minimize the user setup time. (E.g. if EWS IIS Auth Setting is set to allow only NTLM, then select only NTLM above for an optimal setup experience.) If none are selected above, default Exchange setting will be used. Do not check any of these options if using client-based authentication.

h. **EXCHANGE WEB SERVICES SETTINGS**

Disable Exchange Web Services - When set to "true", client will disable all Exchange Web Services activities including calendar forward and calendar attachment.

Exchange Web Services URL endpoint - Specify the Exchange Web Services URL endpoint. (Example: https://mydomain.com/EWS/Exchange.asmx)

i. **EXCHANGE ACTIVE SYNC SETTINGS**

Default Domain - Windows NT Domain to try automatically when logging in. If your server uses newer UPN (email@host.com) style login instead of the older (domain\user) style login, this field should be omitted.

Active Sync Server - Specify the default Exchange Server used to attempt to connect. (Example: cas.mydomain.com)

Auto Discover URL - Provide auto discover URL if known. This will speed up the auto discover setup process. (Example: https://autodiscover.mydomain.com)

Auto Discover Connection Timeout in Seconds (iOS only) - Auto discover connection timeout in seconds.

j. **ADVANCED SETTINGS**

Specify additional configuration parameters in this text area. Contact BlackBerry Support for more details.

8. Click the **Advanced Configuration** tab to configure the following:

a. **ACTIVESYNC USER NAME FORMATS (IOS ONLY)**

Select the User Name Formats to be used to authenticate with Exchange ActiveSync Server. If only certain User Name Formats are supported from Exchange, set those values to minimize the user setup time. (E.g., if ActiveSync IIS Auth Settings are set to allow only SMTP but not UPN, then de-select UPN in the app setting.) If none are selected, authentication with all User Name Formats will be attempted.

Choices are UPN, Domain/UserId, and SMTP.

b. **EXCHANGE WEB SERVICES USER NAME FORMATS (IOS ONLY)**

Select the User Name Formats to be used to authenticate with Exchange Web Services. If only certain User Name Formats are supported from Exchange, set those values to minimize the user setup time. (E.g. if EWS Auth Settings are set to allow only SMTP but not UPN, then de-select UPN in the app setting.) If none are selected, authentication with all User Name Formats will be attempted.

Choices are UPN, Domain/UserId, and SMTP.

c. **EXCHANGE TLS CERTIFICATE SETTINGS**

Specify the User Credential Profile Name for the TLS certificate to be used for Exchange connection. Enter the User Credential Profie Name exactly as entered in UEM Console.

d. **EMAILSYNC WINDOW**

Enter the maximum email sync window allowed. There is no limit.

Note: Users will still be able to select any value less than the entered maximum.

Decreasing the maximum value may overwrite a user's current setting. In turn it may soft delete emails outside of the applied sync window from the Work app.

Increasing the maximum value will not increase the user's current setting. The user will have to increase it manually if needed.

e. **EXCHANGE ACTIVESYNC 16.0 PROTOCOL (BETA)**

To enable (set to "true), check the checkbox for "Use EAS 16.0 protocol."

When set to "true", the client will use Exchange ActiveSync 16.0 protocol for sync if the Exchange server supports it. Otherwise the client uses EAS 14.1 or lower protocols. NOTE that changing this setting will cause the client re-sync all data from Exchange server.

f. Shared Mailboxes

Select the Enable access to Shared Mailboxes option if you want to allow users to add a shared mailbox that they are a delegate for in BlackBerry Work. If this option is disabled after shared mailboxes have been added, existing shared mailboxes are removed, and they are not restored if the setting is enabled again. Also, if a user attempts to add a shared mailbox when this option is disabled, they will not be able to add the mailbox and will see a message in the BlackBerry Work app stating that they must contact their administrator.

g. **OFFICE 365 SETTINGS**

Click checkbox for "Use Office 365 Settings" to use Office 365 Setup Configuration for Work mailbox account

setup.

Click checkbox for "Use Office 365 Modern Authentication" to use Office 365 Modern Authentication when logging into Work mailbox account.

Enter an Office 365 Sign On URL. If left blank, Work setup will try https://login.microsoftonline.com during an initial setup.

Enter Office 365 Tenant ID. If left blank, Work will use "common" during an initial setup.

Enter the Application ID registered in your Azure Portal.

9. Click **Update** to save your changes. Remember, you can always return to modify these settings and/or create different policy sets pertinent to the user groups you create.

Setting BlackBerry Work Security Policies

Policy sets contain rules that govern the security of GD applications and rules specific to the devices and OS versions configured in Good Control. These rules include policies for application passwords (Application passwords), fingerprints use (Fingerprint policies), lock screens, wearables (– BlackBerry Work for Android Wear), authentication delegation (Authentication Delegation), data leakage prevention, certificate management, provisioning (access keys), and agreement message.

To set policies in these areas, in the Good Control console navigator (left-hand panel) click **Policy Sets**, select a policy to clone and/or modify by clicking it, then click the **SECURITY POLICIES** tab. Explanations for available policy settings are provided on the Security Policies page.

Application passwords

You have the option of forcing use of an application password or requiring no password for BlackBerry Work for iOS and/or Android devices. Check the appropriate checkbox at the top of the Password Policies secton to require or not require use of a password.

If you force use of a password, you can:

- Specify an expiration date for the password
- Disallow previously used passwords
- Set a minimum number of characters required
- Allow at most a specified number of occurrences of any given character
- Not allow more than one password change per day
- Require both letters and numbers
- Require both upper and lower case
- Require at least one special character
- Not allow more than two numbers in sequence
- Not allow personal information

Fingerprint policies

To set the fingerprint policies for BlackBerry Work:

1. In the Good Control console navigator (left-hand panel) click **Policy Sets**, select a policy to clone and/or modify by

clicking it, then click the **SECURITY POLICIES** tab.

2. Choose to enable iOS Touch ID or Android Fingerprint BlackBerry Work idle unlock. Default for both is disabled.
3. Checking the enable box for a device type causes two extra options to be displayed:

   Enable the option also for a device cold start (weakening system security and allowing the possible disclosure of user credentials.

   Force password re-entry after a time that you specify, from one hour to seven days. Default is one day.
4. Click **Update** to save your changes. Remember, you can always return to modify these settings and/or create different policy sets pertinent to the user groups you create.

Authentication Delegation

The BlackBerry Work app can delegate its user authentication to other BlackBerry Dynamics or Good For Enterprise applications running on the same device. An application that handles authentication for other BlackBerry Dynamics applications on a device is called the **authentication delegate** or **authenticator**.

Prioritizing Delegation

A prioritized set of up to three applications can be authentication delegates. This is called "multi-authentication delegation." During authentication, each is tried in turn, starting with the primary and ending with the tertiary application you specify. In addition, you can set a "fallback" delegate when all specified delegates have been tried without successful authentication. The fallback delegate is the app itself. If no authentication delegates have been set, the system default is that the application is its own delegate.

Any BlackBerry Dynamics or GFE application can be designated as an authentication delegate. Applications that serve as authenticators must be based on the latest BlackBerry Dynamics SDK for iOS or Android, must be registered (see Adding Applications and Users), and must have a native bundle ID. In Android, this is the app's **package** name and in iOS the value of the **Bundle** keyword in the app's plist file).

When authentication delegation is enabled, users included in this policy set must have the authenticator application installed and provisioned on their devices in order to use any other BlackBerry Dynamics applications. If one of these users launches a BlackBerry Dynamics application, the device displays the password screen for the authenticator application instead of the application they are attempting to launch. Only after entering the password for the authenticator is the user allowed to access the application they had originally tried to launch. In essence, the user enters the same password for multiple BlackBerry Dynamics applications, because all the applications pass their authentication to the authenticator application.

If the user deletes the authenticator application from a device, the user can no longer access *any* other BlackBerry Dynamics applications on that device, unless self-authentication fallback by an application itself has been enabled, as described above. To remedy this, the user can reinstall the authenticator application.

Assigning Authentication Delegates

To assign authentication delegates for a policy set:

1. Click **Policy Sets** in the navigator, then click the desired policy you want view/modify. The **SECURITY POLICIES** tab opens by default. If not, click it.
2. Scroll down to **Authentication Delegation** and click **Add Application** to display the list of currently registered

applications.

3. Click the plus sign associated with each app you want to act as a delegated authenticator on the devices of all users assigned the policy set.
4. After you have added the desired delegates, use the up and down arrows to change the priority/precedence of the delegates. For each user covered by this policy, **Primary** is attempted first, then **Secondary**, and so forth. In general, you should avoid naming multiple auth delegates that are available in the same platform. Specify multiple auth delegates if the primary auth delegate is not available in all of your target platforms (e.g., Mac OS).
5. Enable **Allow self-authentication when no authentication delegate application is detected** as the fallback authentication mechanism on devices that do not have any delegates installed.
6. Click **Update**.

Tip: Although BlackBerry does not recommend a one-size-fits-all model—meaning your IT group must implement the scheme most appropriate to your environment—where GFE is in already in use, BlackBerry Work should be set as the primary authentication delegate, BlackBerry Access as the secondary authentication delegate, and GFE as the tertiary delegate.

Overriding Short Setup

If you want to override the short setup for user activations, you can configure the BlackBerry Work app in Good Control to take the user directly to the long form; i.e., activation requiring an authorized Active Directory username, password, and domain to activate the user's enterprise email account for BlackBerry Work on the device.

To override short setup and take users directly to the long form, in the Configuration JSON, add "skipShortSetup":"true"

Disabling EWS Features

Enabling/disabling EWS only works at the global level, not the domain level. Therefore, care should be exercised when configuring this setting is a multi-domain environment.

To disable EWS features:

1. Click **Manage Apps** under **APPS** in the Good Control Dashboard.
2. With the **ENTERPRISE** tab open, search for or scroll down to **BlackBerry Work**.
3. Click the **BLACKBERRY DYNAMICS** tab.
4. In the **Server** section, click **EDIT**.
5. Add the JSON parameter **"disableEWS":"true"** to disable EWS features to clients. Make the value **"false"** to restore EWS features.

Click **Save**.

Setting Up Support for Creating and Joining a Skype for Business Meeting

This version of BlackBerry Work supports the ability to create Skype meetings from the Calendar app directly in Skype for Business and the ability to join Skype for Business meetings directly from Event View in the Calendar app. A new Join

button opens the Skype for Business app on the user's device.

Skype for Business is the new name for Lync (beginning with Lync 2015).

Prerequisites for Calendar support for Skype for Business:

- One of the following supported environments:
  - Ex 2016 (on-prem) + Skype for business 2015 (on prem)
  - Ex 2010 (on-prem) + Skype for business 2015 (on prem)
  - Ex 2013 (on-prem) + Skype for business 2015 (on prem)
- The Skype for Business client must be present on user devices in order for users to join Skype meetings (but not to create them)..
- Android and iOS devices are supported.

To configure support for Skype for Business perform the following steps:

1. Create and configure a user account on the Exchange 2016 sever, if one does not yet exist.
2. Create and configure a user account on a Lync sever.
3. Ensure that the following DNS names are added to the DNS controller on the Windows Server:
   - lyncdiscoverinternal.<domain> and/or lyncdiscover.<domain>
   - meet.<domain>.
   - For details, refer to:
     - https://technet.microsoft.com/en-us/library/dn951375.aspx
     - https://technet.microsoft.com/en-us/library/dn951397.aspx
4. Set up the desired communication protocol on the Exchange sever: PKINIT, Kerberos, etc., if not yet configured.
   - To set up PKINIT authentication on an Exchange server, follow the Microsoft guide at https://technet.microsoft.com/en-us/library/mt791265(v=exchg.160).aspx. To enable PKINIT authentication, update the GD JSON configuration file: "useEASAuthCert": "true" , "EASUseSSL": "true". To create a PKINIT certificate, you'll need a Windows machine with a user who can log in to the domain.
5. Set up the desired communication protocol on GC: PKINIT, Kerberos, etc., if not yet configured.
   - To enable kerberos authentication, update the GD JSON configuration file: "useKCD": "true"
6. Enable Skype in a GC policy (Policy->APPS->App Specific Policies->Blackberry Work->Interoperability->Skype for Business).
   - Check "Allow creation of Skype for Business meetings in Calendar." This adds the option for a user creating a new Calendar event.
   - Check "Allow launch of the native Skype for Business app" to enable users to join Skype meetings from Calendar.
   - Enter the fully qualified domain name for the Skype for Business meeting links. This is the URL used when users use the "Join meeting" button in an Calendar event's details.

     Note: (iOS) Policy settings that you make in Interoperability under "Launch 3rd Party App" do not affect the Skype for Business feature in Calendar.
7. Log in to the Skype for Business app on a user device. Install a certificate on the device if required.

   To generate PFX certificates for users:

   a. Connect with the CA (Certificate Authority) server using IE (recommended), using your admin credentials.

b. Choose: Request a certificate --> Advanced certificate request --> Create and submit a request to this CA.

c. In the Certificate Template field choose the template you have created for Skype For Business use.

d. To install this certificate, in IE go to Internet options --> Choose Content --> Certificates --> Export desired certificate as PFX file with password to local disk.

e. Upload the certificate from the path where it was saved to the user's email account on GC.

To generate a CER cert for root certificates, for use by GC:

a. Go to Internet options in IE --> Choose Content --> Certificates --> Export desired certificate as CER file to the local disk,

b. Upload the CA certificate: MMC --> Certificates --> Trusted root certificates --> Export CA certificate for domain controller --> DER (CER file)

c. Go to GC --> Certificates --> Upload new certificate (use DER).

8. Try out Skype for Business with Blackberry Work by tapping the Join Skype link in Calendar to launch Skype for Business and join a meeting.
9. To create a Skype meeting using OWA/OL, refer to https://support.office.com/en-us/article/Set-up-a-Skype-for-Business-meeting-in-Outlook-b8305620-d16e-4667-989d-4a977aad6556.

Skype limitations:

- The Lync account and Exchange must be in the same domain.
- Skype for Business does not support shared calendars.

Troubleshooting

When encountering problems while creating or joining a Skype meeting in BlackBerry Work's Calendar app, first check the Networking Skype section in the device BlackBerry Diagnostics feedback.

Some specific problems:

1. Error 502 - This is a BlackBerry Proxy server error, to be addressed by the server's administrator.
2. Error 400 and Only Discovery URL - Confirm that the user has been added to the Skype for Business pool in the Skype server.
3. Error 401 - Access Forbidden - Try a manual sync, and then create the Skype for Business meeting again. If this doesn't help, the problem may be caused by hybrid account problems.
4. If a new meeting does not appear in the Skype for Business list, check the number of meetings in Skype for Business. A maximum of 50 meetings will be displayed. Otherwise, connect with VPN and add any required certificates to the device.
5. If a user can't log in to Skype for Business or can't create a meeting, or if an error occurs, connect with VPN and add any required certificates to the device.

Enabling Exchange ActiveSync (EAS)

EAS is a protocol designed for the synchronization of email, contacts, calendar, tasks, and notes from a messaging server to a smartphone or other mobile device. The protocol also provides mobile device management and policy controls.

Please ensure that Exchange EAS is enabled on port 443 and that connections are permitted to the Good Proxy server.

By default, ActiveSync is enabled when you install the Client Access server role on the computer that's running

Microsoft Exchange Server 2010.

Prerequisites include:

- The Internet Information Services (IIS) component ASP.NET is installed.
- The ASP.NET Web service extension status is **Allowed**, not **Prohibited**. You can verify the status of the ASP.NET Web service extension in IIS Manager by expanding the server name and clicking **Web Service Extensions**. If the ASP.NET Web service extension isn't set to **Allowed**, right-click the Web service extension to change its status.

Use IIS Manager to enable EAS with the following steps:

1. Click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. Double-click to expand the server name, then expand the **Application Pools** folder.
3. Right-click **MSExchangeSyncAppPool**, and then click **Start** to enable ActiveSync.

Note: If the **Start** command isn't available, then ActiveSync is already enabled on this server.

Configuring Exchange Autodiscover

Autodiscover is a Microsoft protocol used to automatically discover specific resource endpoints. This protocol is used by many Microsoft products, including Exchange. See "Autodiscover for Exchange" for additional details on the protocol and the autodiscover process.

BlackBerry Work can be configured to use Autodiscover to automatically discover its Exchange ActiveSync server. If you plan to use Autodiscover for BlackBerry Work, you will want to consider the following as it pertains to your environment:

1. **Exchange On-premises Environment** – the autodiscover URL (**autodiscover.mydomain.com**) should point to one of your Exchange CAS servers. If you are using a load balancer (LB), point the URL to the LB and then route it to your group of CAS servers.
2. **Exchange On-premises Mixed Environment** – in this case you have a combination of Exchange 2010 and 2013 servers. The autodiscover URL should point to the higher version Exchange CAS servers.
3. **Exchange Office 365 Environment Only** – autodiscover URLs are typically handled by Microsoft. although if you've migrated your domain to O365, make sure your domain autodiscover URL (**autodiscover.mydomain.com**) points to Microsoft's master autodiscover URL—**autodiscover.outlook.com**. On your DNS admin portal, make sure a **CNAME** record is created and that it points **autodiscover.mydomain.com** to **autodiscover.outlook.com**.
4. **Exchange Office 365 Hybrid Environment** – in a hybrid environment, mailboxes can exist in both on premise and the O365 cloud. The domain autodiscover URL should point to the hybrid Exchange server.

> **Important:** All autodiscover URLs must be whitelisted on the Good Control server and be resolvable from the Good Proxy server. Independent of BlackBerry Work, you can use the Microsoft RCA tool or the EWSEditor tool to test autodiscover. For more information, please see KB5558.

Implementing KCD for BlackBerry Work

When correctly configured with the appropriate environmental settings, Kerberos Constrained Delegation (KCD) allows the provisioning of the BlackBerry Work application[1] without requiring users to enter their Active Directory password.

Very briefly, here's how it works.

A Kerberos client (a user or a service) sends requests for tickets to the Key Distribution Center (KDC) in the domain. Requests for ticket-granting tickets (TGTs) are sent to the authentication service of the KDC, and requests for service tickets are sent to the ticket-granting service of the KDC. When a client sends a request to the authentication service with credentials that can be validated, the KDC returns a TGT to the client. This TGT is issued for a specific client and can be reused by the client in requests for additional service tickets for the same service. A client must obtain a new TGT from the authentication service before it can obtain service tickets for another service. Each service ticket issued by the ticket-granting service is for a specific service on a specific host computer.

[1] The GEMS Docs service does not currently support Kerberos Constrained Delegation.

That said, the Kerberos protocol includes a mechanism called delegation of authentication. When this mechanism is used, the client (the requesting service) delegates authentication to a second service by informing the KDC that the second service is authorized to act on behalf of a specified Kerberos security principal—in the case of BlackBerry Work, a user that has an Active Directory directory service account. The second service can then delegate

authentication to a third service.

This is achieved by setting the service account running the Good Control service to be a trusted authenticator within Active Directory. Configuration requires setting appropriate Service Principal Names (SPNs) and configuring the ActiveSync virtual directories on Exchange to accept Kerberos Authentication as an allowed mechanism.

For environments where a Layer 7 load balancer is utilized in front of the Exchange servers holding the ActiveSync virtual directories, further configuration is required to set the HTTP service to run as an Alternate Service Account, a separate SPN set for the Active Sync URL FQDN, and mapping this SPN to the Good Control service account under which it will run as a service.

Environments Supported

See the Mobile/Desktop OS and Enterprise Applications Compatibility Matrix.

Additional Requirements

In addition to one of the supported environments listed above, the following steps must be taken to properly implement Kerberos Constrained Delegation for BlackBerry Work:

- KCD Authentication must be enabled on all EAS virtual directories in Exchange
- KCD must be correctly configured and enabled in Good Control

Limitations

The following currently comprise the known limitations with respect to implementing KCD for BlackBerry Work:

- Because BlackBerry Work KCD relies on Good Control KCD, it is subject to the limitations of Good Control KCD
- BlackBerry Work KCD is supported with either:
  - a hardcoded **EASServer** value in the BlackBerry Work JSON configuration; or
  - an **AutodiscoverURL** in the JSON configuration.

  Either way, however, **Negotiate authentication** must be configured for EWS virtual directories or Autodiscover virtual directories, respectively. For details, see Exchange Virtual Directory Settings.
- BlackBerry Work KCD does not support fallback when KCD authentication fails.

For a more extensive description of KCD and its features, benefits, and operating principles, please see Microsoft's *Kerberos Constrained Delegation Overview* in TechNet. To learn more about how KCD operates with BlackBerry Dynamics, consult the official BlackBerry Dynamics guide on *Kerberos Constrained Delegation*.

Otherwise, proper setup and configuration of KCD authentication for BlackBerry Work consists of three (3) major phases in the following sequence:

1. Preparing your environment for KCD
2. Creating the IIS Alternate Service Account for load balancing
3. Configuring delegation to Good Control.

Preparing Your Environment for KCD

As you proceed, keep in mind that, as of Exchange 2010, clients no longer connect directly to the Information Store on the Mailbox server role to access mailbox data. Instead, clients connect to a set of services on the Client Access Server

(CAS) role, and services within the CAS role then access mailbox data from the Mailbox server on behalf of the connecting user.

To set the appropriate environmental parameters that will support KCD, you will need:

- the correct domain
- a Windows Service Account (**blackberryadmin** is recommended)
- FQDN of the Good Control server
- URL for the ActiveSync Virtual Directory
- Client Access Array Name

If you are implementing L7 load balancing, you will also need to have ample CAS machines residing behind HWLB.

To configure your environment for KCD:

1. Run the following command from a Domain Controller to set the SPN for the Good Control Service (GCS):

   ```
   C:\>setspn -a GCSvc/<fqdn_of_gchost> <your_domain>\blackberryadmin
   ```

   > **Note:** In newer versions of Windows Server (e.g., Windows Server 2012), the **-a** option may need to be replaced with the **-s** option. The **-s** parameter verifies that no duplicate SPNs exist before adding the new SPN.

2. Next, create the keytab file by running:

   ```
   C:\>ktpass /out gdadmin.keytab /mapuser blackberryadmin@<your_domain>
   /princ blackberryadmin@<your_domain> /pass <password> /ptype KRB5_NT_PRINCIPAL
   ```

   This saves the **gdadmin.keytab** file to the directory on the server from which you ran the command.

   > **Important:** *<your_domain>* name must be in all capitals. The password must be the password for your **blackberryadmin** service account, if you change the password for this service account, this keytab file will have to be recreated.

3. Copy the **gdadmin.keytab** file created in the above over to the **C:\good** directory on your Good Control server.
4. Now, set the appropriate values in the Good Control console.
   a. In the navigator under **SETTINGS**, click **Servers**.
   b. Open the **Server Properties** tab and, for each of the following properties, enter the value indicated.

Property	Value
gc.krb5.enabled	☑
gc.krb5.kdc	*<FQDN of your domain controller>*
gc.krb5.keytab.file	*<path to the gdadmin.keytab file>*
gc.krb5.principal.name	*<service account name in all CAPS>*
gc.krb5.realm	*<domain name in all CAPS>*

> **Important:** Use forward (tick) slashes for the **keytab.file** path name; ex: **C:/good/gdadmin.keytab**.

5. Next, on each CAS machine which holds the ActiveSync virtual directory, open IIS and select the **Microsoft-Server-ActiveSync** virtual directory, then:
   a. In the far right panel, click **Authentication** under **Actions**. Then, assuming Windows Authentication is enabled, select **Providers...**
   b. In the **Providers** window, click **Add**.
   c. From the list of **Available Providers**, select **Negotiate:Kerberos**.
   d. Click the **Move Up** button until **Negotiate:Kerberos** is at the top of the list of **Enabled Providers**.
   e. Click **OK** to save this setting.

You are now ready to create the IIS alternate service account for your load-balanced Client Access servers (CAS).

Creating the IIS Alternate Service Account

In order to use Kerberos authentication with load-balanced Client Access servers (CAS), you need to complete the configuration steps described in this topic. For more detailed guidance from Microsoft on cross-forest scenarios, please see *Configuring Kerberos authentication for load-balanced Client Access servers*.

You use Active Directory Users and Computers (ADUC) to manage recipients. ADUC is an MMC snap-in that is a standard part of Microsoft Windows Server™ operating systems, extended to include Exchange-specific tasks.

To create and configure the IIS Alternate Service Account (ASA):

1. From ADUC, create a service account; e.g., **`myblackberry\f5service`**.

> **Note:** This account needs no permissions or elevated rights.

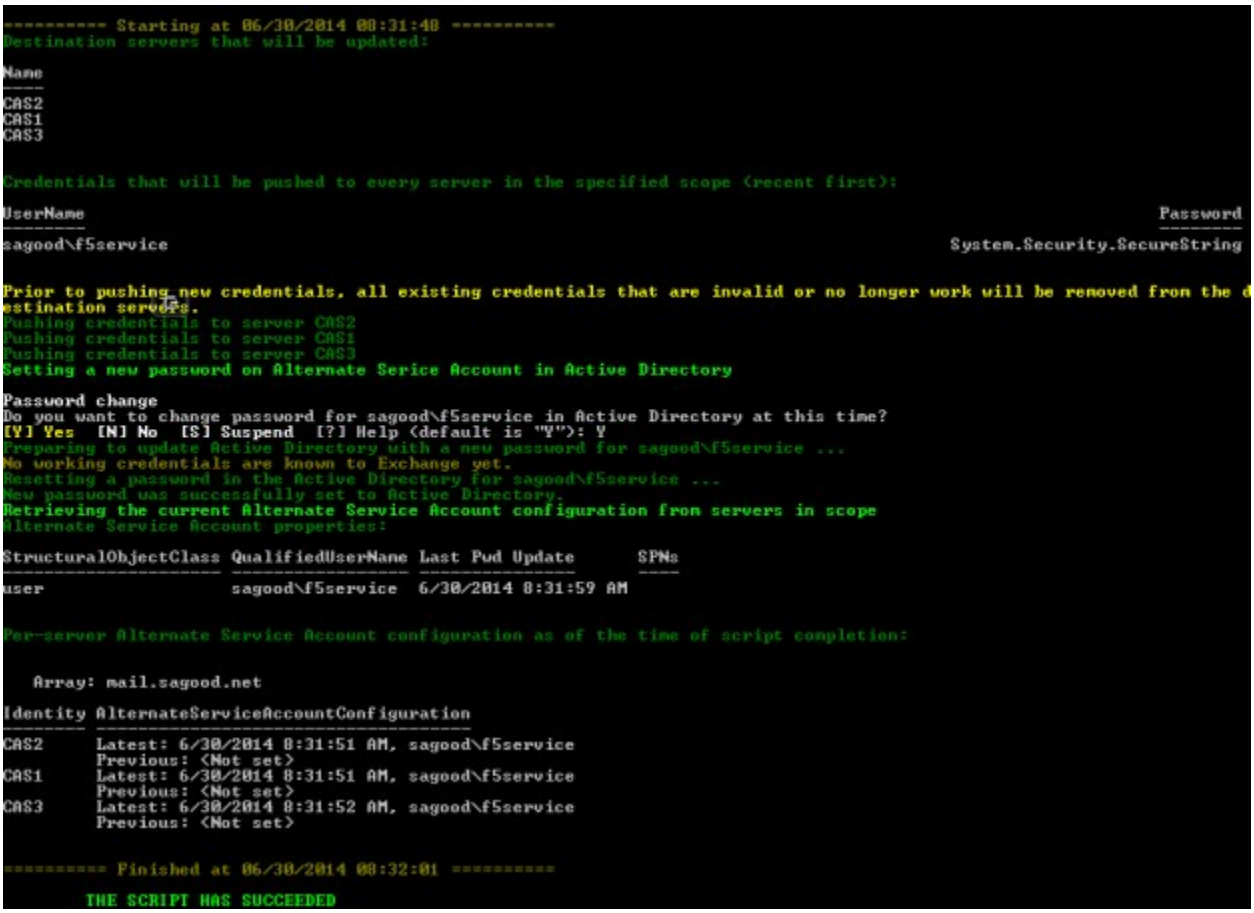
2. From an Exchange server within your organization, login as an administration and open Exchange Management Shell, then browse (**cd**) to the scripts directory located in:

   C:\Program Files\Microsoft\Exchange Server\V14\Scripts

3. Run the following script:

```
RollAlternateServiceAccountPassword.ps1 -ToArrayMembers <fqdn_of_client_access_array>
-GenerateNewPasswordFor myblackberry\f5service
```

The output will look something like the screen captured below but with information and machine names pertinent to your environment.



When complete, output ends with "**THE SCRIPT HAS SUCCEEDED**."

4. Verify this by running the following cmdlet:

```
C:\>Get-ClientaccessServer -IncludeAlternateServiceAccountCredentialStatus |
fl name,alter
```

5. Now set the SPN for the FQDN used above by specifying the ASA name with the following command:

```
C:\>setspn -S http/<fqdn_of_client_access_array> myblackberry\f5service
```

This registers the Service Principal Name.

6. Next, perform a resest on all CAS machines within the organization with this command:

```
C:\Windows\system32>iisreset noforce
```

You are now ready to delegate authentication to Good Control.

Configuring Delegation to Good Control

As previously discussed, delegation is the act of allowing a service to impersonate a user account or computer account in order to access resources throughout the network. When a service is trusted for delegation, that service can impersonate a user so that it can use other network services.

To set up delegation to Good Control, the following conditions must be met:

- The account doing the delegation must be set to **Trusted for delegation to specified services only**.
- The account that the service is delegating for must not have the **Account is sensitive and cannot be delegated** option chosen.
- An administrator must have the **Enable computer and user accounts to be trusted for delegation** privilege on the computer in order to enable delegation.

To configure authentication delegation to Good Control:

1. From **ADUC**, select **View**, select **Advanced Features**, then click **Users**.
2. Double-click the service account running the Good Control service (e.g., **blackberryadmin**) and open the **Delegation** tab.
3. Enable **Trust this user for delegation for specified service only**.
4. Select **Use any authentication protocol**.
5. Click **Add**.
6. Select each CAS server that holds a virtual directory. Or, in the case of a single CAS server select the single CAS server machine name. Pictured in the example below, **CAS1**, **CAS2** and **CAS3** machines hold the ActiveSync directories.
7. Next, click **Add Services** and select all **HOST**, **http**, and **www** services related to each of the CAS servers in your organization.
8. Click **Add...** again and then input the service account name; in this case, **blackberryadmin** , then click **Check Names**.
9. From the list of **Available Services** you should see **GCSvc** with the FQDN of your Good Control server that was created in Step 1 under Preparing Your Environment for KCD above.

> **Note:** Steps 10 and 11 below are only applicable if you are using a CAS array. If you are not using a CAS array, skip to Step 12.

10. Click **OK**, then enter the name of the service account you created in Step 1 of Creating the IIS Alternate Service Account above.
11. When presented with the Service Type **http** corresponding with the FQDN you specified in Step 3 of Creating the IIS Alternate Service Account above, click **OK**.
12. The list of specified services displayed should now allow Kerberos Constrained Delegation for the BlackBerry Work application against ActiveSync virtual directories when using a HWLB with Exchange 2010.

    Click **Apply**, then click **OK**.

> **Note:** The sequence for configuring KCD for Exchange 2013 is virtually indentical, with only some minor variations.

Configuring the BlackBerry Work App for KCD

The final part of the KCD configuration process for BlackBerry Work is enabling KCD in the BlackBerry Work application settings in Good Control. This simply requires a short block of JSON appended to what's already in place for EAS or Autodiscover.

To add the JSON for KCD:

1. Under **APPS**, click **Manage Apps**, search for or scroll down to **BlackBerry Work** and click it.
2. Click the **BLACKBERRY DYNAMICS** tab, then, in the **Server** section, click **EDIT**.
3. Add/append the following JSON to the existing configuration (open and close brackets are not needed if already present).

```
{
   "useKCD":"true"
}
```

With this JSON parameter added, the **Configuration** field should look similar to this:

> **Note:** Currently, **useKCD** is only supported when the **EASServer** parameter is set.

4. Click **Submit** to save your changes.

Setting Up S/MIME

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of MIME data to ensure even more robust authentication, message integrity, and non-repudiation of emails sent and received using S/MIME-configured BlackBerry Work clients.

For additional details and guidance, see the SMIME sections in the product guide supplemental *Client Certificates for BlackBerry Work for Good Control*.

Device Verification and Testing

The BlackBerry Work app is publicly available from the Apple App Store or the Google Play store. By default the app will only use HTTP/S to communicate with GEMS when it registers for push notifications. If you would like to do device verification and testing in a test environment, you can configure communications to use HTTP instead of HTTPS.

This is a matter of making additional changes to the Good Control configuration (JSON) we set up when configuring the BlackBerry Work app with Active Sync earlier.

If you haven't already done so, download the BlackBerry Work app to your device.

Upon launching the BlackBerry Work app for the first time, you will be prompted for an email address and a provisioning PIN. If you don't have this information, refer to the previous section on device activation keys.

BlackBerry Work will continue the provisioning process once the email address and PIN is entered correctly. Depending on the Good Control policy for the device, you may be prompted to create a password for the app. After the app password is set, you will be prompted for your enterprise email address and Active Directory password. If the system is not able to correlate your email address to an Exchange Active Sync (EAS) server, you will be prompted for a different EAS server and domain credentials.

When everything is setup correctly, BlackBerry Work will automatically start synchronizing with Exchange and you will start to see mail, calendar and contact information in the app. If BlackBerry Presence is configured, you will also see presence information for each contact.

Device Provisioning and Activation

Users invited to install and activate BlackBerry Connect on their device(s), require an access key. The access key must be entered when the user opens BlackBerry Connect for the first time on a given device.

The access key is a 15-character alphanumeric code sent to the user's (registered) company email address and has the following properties:

- It can be used only once and is consumed immediately upon the activation of an application.
- It is not application-exclusive. In other words, a user who has been sent four access keys can use them to activate any four applications to which s/he is entitled.
- It does not support reactivation. Hence, if the client software is uninstalled, then reinstalled on the same device, a new access key is required. This is also true if a new or factory-reset device is in use, or if a device emulator is in use and its state is not persisted. However, a user who has been issued multiple access keys could use them to activate the same application multiple times.
- It can be configured to expire after a specified period of time. This is done in **Provisioning Policies** under the **SECURITY POLICIES** tab by enabling the **Access Keys expire** option, and then selecting the number of days after which access keys expire if not consumed.

To grant access to all your enterprise users complete the following steps:

1. Assign the default policy set or create a new policy set in accordance with your enterprise's user access protocols. The default policy set is automatically applied to all new users.

   For each user, the policy currently applied is located at the top of the user's account page. To apply a different policy set, hover your cursor over it and select from the available policy sets in the listbox. It should be noted that the user must be granted access to the app in order to activate it. This is done by assigning the user to an App Group that includes the app (BlackBerry Work) for which the user is being permitted access.
2. Go to **USERS > Users and Groups** in the navigation panel, locate and select the user you want to provision by clicking the corresponding checkbox, then select **Edit** from the **User Actions** listbox.
3. Click on the **Keys** tab, then click **New Access Key**.

A new access key will be sent to the user's registered enterprise email address—one email message per key. Hashes of

the access keys are also copied to the GD NOC for validation.

Assuming the user has received the email message containing the access key and downloaded and installed the GD client application from the pertinent online marketplace—App Store or Google Play—on the device, they can now activate the application until its GC-specified expiration date. At application start-up, the BlackBerry Dynamics user activation interface opens, whereupon the user must enter the access key and his/her enterprise email address in the input fields provided on the client so that the GD Client Library can promptly transmit the access key to the NOC.

Additional provisioning and activation options are also available in Good Control.

Appendix A – Content Synchronization and Notifications on iOS

By definition, a push notification is a message or alert delivered by a centralized server to an endpoint device. The primary benefit of the notification system is to improve the user experience of synchronization while the application is in the background on iOS. In BlackBerry Work, this allows the server to instruct the client to start synchronizing. The client, in turn, can then receive email messages and notify users of any new messages available by displaying a message in the iOS Notification Center—all while BlackBerry Work is in the background.

BlackBerry Work is able to provide this support for timely content delivery and notification on iOS devices by taking advantage of several operating system features; namely, APNS, Background Processing, and Banner/Badge Updates.

The balance of this appendix offers insight into the expected behavior and certain limitations of the mechanism in terms of:

- Initial setup
- Foreground operation
- Background processing
- Badge count updates
- VIP notifications
- Scenarios and behaviors
- Troubleshooting

Foreground Operation

After initial setup, the device is now configured to receive push notifications while the client is unlocked and in the foreground. This provides one major benefit over standard "long-poll ActiveSync" or "pull" based notifications in that updates and deletes are *pushed* immediately to the device by GEMS.

Background Processing

At this point the device is setup and push notifications are working in the foreground. When subsequently placed in the background—e.g., the phone screen is turned off or the user switches to a different application—BlackBerry Work is designed to intelligently continue synchronizing the email inbox, as well as calendar changes, and present local notifications to the user.

The iOS platform itself, however, imposes a number of limitations on all applications, including:

1. **Applications are suspended after approx. 1 minute in the background**. Unlike Android, iOS will "suspend" BlackBerry Work 30 to 60 seconds after the user puts it into the background. Apple does this to promote better performance and battery life for the device.
2. **Applications are "woken"—unsuspended or resumed—only periodically**

   Delivered through the NOC (#3 in the diagram above), BEMS sends a notification to Apple's push servers (#4)every time there is a change. Once Apple delivers the notification, the device (#5) itself may not queue up the messages. At this point, Apple may queue or dump the messages altogether based on factors (currently undocumented by Apple) including connectivity of the device (Wi-Fi, cellular), volume of notifications, and device battery level.

3. **Applications only get brief amounts of time when resumed in the background**

   There will be instances in which, even after receiving a notification, iOS may not wake up the app. This is because, barring user action, BlackBerry Work remains up for a maximum of 30 seconds. Hence, if the user's mailbox reports multiple updates on Exchange before BlackBerry Work has been launched on the device for a significant period of time, all new information may not have been processed sufficient to wake up the app.

   Furthermore, the scale of emails synchronized is predicated on how long iOS remains active after it wakes up BlackBerry Work. If there are many updates on Exchange and the app has not been launched for several days, then it is highly likely that the updates/deletes have not made their way to the device and thus the badge count can be expected to be off.

   What this means is that the badge count is calculated by BlackBerry Work, so if there are many updates on Exchange and the app has not been launched for several days, then the badge count may not be up to date with the Outlook unread count.

   Bottom line: Launching BlackBerry Work regularly is the best way for heavy volume users to stay up to date.

Badge Count Updates

In the previous versions of BEMS and BlackBerry Work (both v1.4), badge count is updated only after the client wakes up in the background and performs synchronization.

With release of BEMS 1.5 and BlackBerry Work 1.5 for iOS, the server-side badge **Unread** count can also have issues if the client is not fully synchronized to the server state before going into the background. This is because the server has no way of knowing how many unread items are/should be on the device. Consequently, only new items received at a given point in time can be obtained.

This makes **New Count** simple—the client resets to **0**, and the server merely sends **1**, **2**, **3**, etc. For **Unread**, it's a bit more involved. Here, the client sends the current **Unread** number for the Inbox and the server begins sending **Unread +1**, **+2**, **+3**, etc. This means the server number will only be as accurate as the base number sent by the client. If the client is not fully synchronized, that number will be off.

It is important that user give the application sufficient foreground time to sync. If the volume is quite high, then insufficient foreground time to sync will result in an incorrect state on the client and be reflected in the Unread badge count. Moreover, if the mailbox is not fully synchronized, no new emails are synchronized, either.

An issue was recently raised surrounding the Unread count wherein the DB size is too large, causing the processing time to be very long and badge counts did not update correctly. This has proven not to be true.

The item to look at is whether the Unread badge count is correct before going to background, then noting when and how frequently that number changes. Currently, it only changes when the app wakes up, performs a sync, and updates the number of unread items.

VIP Notifications

A VIP notification is sent for a message if it is from a designated VIP sender, or meets **VIP rule conditions** as defined here:

1. A user can manage a list of VIP contacts and add/remove VIPs from the contact card.
2. A user can view a list of VIPs in the contacts VIP smart folder. When a new contact is added from within the VIP smart folder contacts group, that contact is directly made a VIP.
3. A user can set preferences on whether the device should play a sound and/or vibrate on receiving an email from a

VIP

4. For Android only – a user can choose the VIP sound alert to override the native device settings; e.g., if the device is set to be silent, an email from a VIP can still play a sound if the preference is set.
5. User will get notifications even if the app is not running/killed.

The scope of VIP notifications is defined as follows:

1. Only messages in the Inbox will be evaluated for VIP.
2. Email sender display name and subject is included in the notification.
3. A server side policy flag controls whether the sender, subject, and first words of message are shown in notifications. This flag is received from the client as a GD policy.
4. The User/App can specify a sound (by file name) in the VIP rule, which will be used for VIP notifications sent due to that rule.

Limitations (Push Throttling):

If multiple messages are received by the user within a short time interval, the device does not "buzz" constantly. Sending many notifications at once also causes degraded battery life on the client. For this reason, notifications are coalesced that occur close together in time under the following conditions:

1. If multiple new messages are received within a 1-minute window, a single push with the alert text "N new messages" is sent.
   a. A new message alert is sent immediately if there have not been any new message alerts in the preceding 1 minute.
   b. After a new message alert has been sent, subsequent new message alerts will be suppressed for the next one minute (coalescing as needed).

Timeouts

1. If no login to the app for 12 hours, BEMS sends generic "Email received" messaged
2. If no login for 3 days, BEMS removes the device registration

In both the cases, pushes resume to normal once the user launches the client to foreground.

Scenarios and Behaviors

As described above there are a number of nuances that impact the overall behavior of push notifications. The following table describes common scenarios and the behaviors that a user would experience.

Scenario	Behavior
User frequently opens BlackBerry Work during the day	APNS tends to deliver notifications in a timelier manner when the application is used frequently
User hasn't used the BlackBerry Work for extended periods	APNS may deliver notifications with delays
User is running many applications or is using an older device	When many applications are running, memory may become low. As this happens iOS stops applications running in the background. If this happens to BlackBerry Work, the user will not receive further notifications until logging in again. The user is notified when this happens: "Offline. To resume sync, open and unlock"
User force kills BlackBerry Work	If this happens to BlackBerry Work, the user will not receive further notifications until launching the application and logging in again
Device just powered up and BlackBerry Work is not started yet	BlackBerry Work will not receive notifications until launching the application and logging in

User receives a number of email messages in a short period of time	BEMS has a mechanism to throttle and batch push notifications to avoid throttling issues with APNS. The default throttle period is 2 seconds, but this is configurable. BEMS will send a single APNS notification for all messages received within the throttle period. The user will then see a notification message that states "N new messages received", where N is the number of messages received in the throttle period. APNS may also batch notifications if too many are received in a short timeframe. This will result in the same notification message as above
User has a large number of new messages to sync to the client while BlackBerry Work is in the background	iOS provides an application 30 seconds to execute while in the background. BlackBerry Work will only synchronize what it can in that time period. The next batch will then be synchronized when the next push notification is received. In most cases, this is not an issue and all new messages are synchronized in one batch
BlackBerry Work crashes while in the background processing a notification	If this rare circumstance occurs, the user will not receive further notifications until logging in again. Starting with our next major release, we will notify the user when this happens "Offline. To resume sync, open and unlock"

Troubleshooting

For most commonly reported issues, take the actions recommended below.

Troubleshooting Initial Setup

After this step, you, as IT admin, should be able to go into the BEMS configuration console and confirm that the push account is configured for the user and that an APNS push key is present. In the device settings for iOS, go into Notifications. The entry for BlackBerry Work should be set to **Allow Notifications** and enable **Show in Notification Center**, **Sounds**, **Badge App Icon**, **Show on Lock Screen** and **ALERT STYLE WHEN UNLOCKED** as appropriate to user preference.

Issue	Resolution
No entry in BEMS present	Verify that the iOS Settings for BlackBerry Work in Notifications are correct. Is BEMS server configured correctly for user? Check the BEMS logs for a registration log entry for the user
No entry for BlackBerry Work in Notifications under Settings in iOS	1. Are you using a build from somewhere other than TestFlight or the Apple App Store?

Issue	Resolution
	YES – Work with whomever provided you the build to make sure that the application was provisioned properly to send notifications NO – Proceed to Step 2 2. Scroll down in the notifications section to "Do Not Include" and look for BlackBerry Work, is it there? YES – Go into that setting and enable push notifications for BlackBerry Work, relaunch the application and allow for the new push information to be sent to the BEMS server, then repeat troubleshooting. NO – Capture device logs and work with BlackBerry Support to resolve

Troubleshooting Foreground Operations

Make sure that initial setup is completed correctly. Login to Outlook as the same user configured in BlackBerry Work. Delete one of the email messages in the inbox. After a short time (generally less than 15 seconds, but environment-dependent), you should see that the email removed from the inbox in Outlook has also been removed from the inbox in BlackBerry Work.

Issue	Resolution
Device always takes longer than 15 seconds to synchronize change	1. Was initial setup completed correctly (device present in BEMS)? NO – Proceed to initial setup troubleshooting YES – Proceed to Step 2 2. Pull to refresh (manually) the email folder; does the change appear? NO – Check network connectivity, troubleshoot synchronization YES – Proceed to Step 3 3. Capture Device and BEMS logs for the time period during a specific attempt and work with BlackBerry Support to resolve
Device occasionally takes longer than 15 seconds to synchronize change	Apple APNS design indicates that push notifications are not guaranteed to be delivered, nor are they always delivered in a timely fashion. Additionally, there could be other synchronization work going on behind the scenes on occasion that would prevent rapid acknowledgement of changes. If this is happening very frequently, then follow the resolutions for "Device always takes longer than 15 seconds", understanding that BlackBerry Work is subject to the limitations of APNS

Troubleshooting Background Processing

Set up the application, verify foreground notification delivery, then place application in background. Send an email to the account being tested. Normally, after a short period of time, you should see the badge count for BlackBerry Work increase and a banner notification displayed.

Issue	Resolution
No notifications are appearing ever	Verify network connectivity, then visit a website in Safari, troubleshoot initial setup, verify that notifications are enabled in BEMS and iOS Settings, as well as properly configured
Only some notifications were delivered	1. Double tap the home button, then look in the task browser for the BlackBerry Work App. Is it present? NO – User force quit application. BlackBerry won't receive notifications or be able to run in background after the user has force quit the application YES – Proceed to Step 2 2. Go into Notification Center (swipe down from top), and look for BlackBerry Work notifications. Is there one asking you to open and unlock the application? YES – Proceed to Step 3 NO – Proceed to Step 4 3. The application was not running, meaning it has been killed in background, either by iOS or an abnormal crash of the application. Check to see if application crash logs are present on the device. YES – BlackBerry Work abnormally crashed. Capture the device logs and the crash log for the incident and send to BlackBerry Support team for troubleshooting. NO – BlackBerry Work was closed by iOS to make room for another application, this is the expected behavior, notifications will resume when app is relaunched and unlocked. 4. If this is happening frequently, capture logs from BEMS and client logs during an occurrence, then work with BlackBerry Support to further troubleshoot

Deploying the BlackBerry Work Client

Three distinct planning phases are recommended to realize a successful GFE-to-BlackBerry Work client migration process. Each is phase can be summarized as follows:

Phase I: Environment Readiness

Prior to deploying the BlackBerry Work client in your environment, make sure the following infrastructure is installed and properly functional.

1. **BlackBerry Dynamics** – The BlackBerry Work client is a BlackBerry Dynamics (GD) app. As such, it requires a Good Control and Good Proxy server. Please ensue that Good Control and Good Proxy are functional in your environment. More information about BlackBerry Dynamics can be found on the BlackBerry Developer Network (BDN) and in the *Good Control and Good Proxy Server Installation Guide*.
2. **Microsoft Exchange** – The BlackBerry Work client uses ActiveSync to connect to Exchange. Therefore, you must ensure that all BlackBerry Work users are enabled for ActiveSync in Exchange. Additionally, make sure the

Exchange server is reachable by the Good Proxy server. More guidance on EAS with the BlackBerry Work client can be found in Appendix C of the *BEMS Administration Guide*.

3. **BlackBerry Enterprise Mobility Server (BEMS)** – BEMS provides extra functionality to the BlackBerry Work client, including Presence, Push Notifications, and more. If you plan to use these extra features and functionalities, ensure that the BEMS host is correctly implemented in your environment. See *BEMS Administration Guide*.

Phase II: Easy Activation

Because the BlackBerry Work client runs on the BlackBerry Dynamics platform, BlackBerry Work users must exist in Good Control before they can activate the BlackBerry Work app on their device. The easiest to achieve this is to rollout the BlackBerry Access secure browser app to all GFE users so that it an be used for Easy Activation.

> **Note:** It is important to remember that, in a GFE deployment, users in Good Mobile Control (GMC) may not necessarily exist in Good Control. This inconsistency presents a problem when using "Easy Activation" with GFE to activate the BlackBerry Work client. However, all BlackBerry Access users already exist in Good Control, making it the logical authentication delegate to apply.

Hence, you can migrate GFE/EWS users via Authentication Delegation and Easy Access using the following procedure:

1. In Good Control, remove GFE as an authentication delegate in each pertinent policy set.
2. Make sure BlackBerry Access is set as the primary authentication delegate.
3. Advise your users who need instant provisioning of BlackBerry Work that they may need to open and close BlackBerry Access a couple of times to force the policy update through on the device.
4. Next, advise your GFE users to download and install the BlackBerry Work app from the appropriate online store—App Store or Google Play—and launch the app.
5. When prompted to provision using either BlackBerry Access or an Access Key, advise your users to choose **Set up using BlackBerry Access**.
6. Remind them to enter their BlackBerry Access password when prompted, and then continue with the remainder of the activation process by following the device's onscreen instructions.
7. If/when you decommission GFE, advise your affected users that they can safely remove the GFE app from their device(s).

Otherwise, please consult BlackBerry Professional Services to customize an automated solution for importing your users from GMC to Good Control.

Initial Setup

Initially, a user provisions and sets up the Good BlackBerry (client) application with their login information, at which point the Good Control (GC) server sends configuration information from BEMS (#2 in the diagram above) to the client. The client (#6 in the diagram above) contacts BEMS to register for push notifications, sending the push token generated by iOS.

Appendix B – BlackBerry Work for Android Wear

Wearable devices to interact and share data offer new avenues for mobile collaboration while also creating a new class of security and privacy risks. For this reason, BlackBerry Work offers limited support for wearable computing.

Wearable computing is broadly classified as anything from your fitness tracker, Google Glass, or any form of computing device that you wear on your wrist, your head, or even clip onto your clothes. Wearable computing devices make it easy for users to go about their daily tasks without worrying that the device is going to get in their way.

Such wearable devices rely on either Bluetooth or Wi-Fi connections to transfer data to a companion app on the mobile device with which it is paired, mainly because it doesn't have a SIM slot to hold its own data. When using a device outside of a controlled wireless network, wearables require higher communications security with respect to encryption, information integrity, and non-repudiation. Since wearable computers are quite small, most do not come equipped with higher security measures baked in, which renders any data sent and received vulnerable.

Consequently, BlackBerry Work's support for wearables is confined to notifications and reminders and, optionally, a corresponding user-initiated voice reply/quick reply enabled via the BlackBerry Work application policy set in BlackBerry Control. The feature includes:

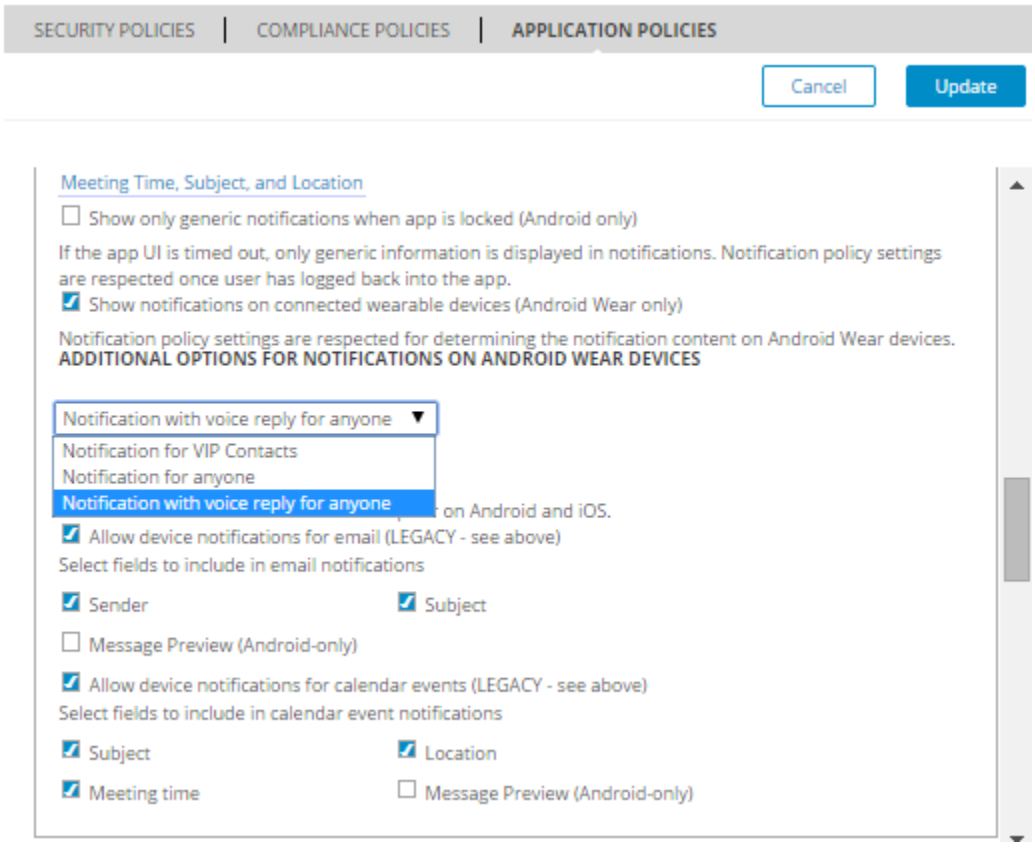
- Single-email notification – voice reply and quick reply
- Multi-email notification – voice reply and quick reply for each email in the notification
- Calendar Event reminders – voice reply and quick reply for emailing invitees
- Meeting Invitation Notification – send Accept/Decline/Tentative

The BlackBerry Work Application Policy in Good Control can be set to:

- Allow/disallow notifications on connected wearable devices
- Allow/disallow voice and quick reply from connected wearable devices

To enable/disable BlackBerry Work for wearables:

1. In the Good Control console navigator (left-hand panel) click **Policy Sets**, select a policy to clone and/or modify, then click the **Application Policies** tab and select **BlackBerry BlackBerry** from the list by clicking it.
2. Click the **Notifications** tab, then scroll down to **ADDITIONAL OPTIONS FOR NOTIFICATIONS ON ANDROID WEAR DEVICES** (pictured).



3. Check/uncheck **Show notifications on connected wearable devices (Android Wear only)** to enable/disable support for Android wearables.
4. From the options listed in the dropdown, make a selection.
5. Click **Update**.

Appendix C – GC Server Configuration Settings and Definitions

This addendum furnishes the standard properties and their format for BlackBerry Work's application server configuration. BlackBerry Work's BlackBerry Dynamics Application ID is **com.good.gcs.g3**.

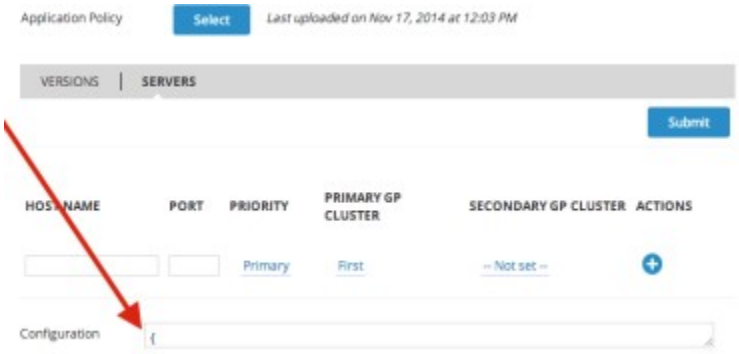
Note: All currently available configuration settings can also be set in Good Control application policies (Setting BlackBerry Work Application Policies). If a JSON setting is present, as described in this appendix, configuration will be taken from JSON. If JSON is not present, the app policy setting will take effect.

Common Guidelines

Configuration options affect the behavior of the app and typically don't require frequent readjustment. The supporting network services and devices described in the core sections of this administration guide should already be set up, tested, and operating properly prior to adding/changing the configuration settings for the BlackBerry Work application server.

Location

Like all BlackBerry Dynamics applications, configuration settings for the BlackBerry application server are found in the Good Control console under **Apps > Manage Apps > BlackBerry Work**.



One example of a BlackBerry Work application server configuration might look like this:

```
{
   "disableSSLCertificateChecking": "true",
   "mycompany.com": {
      "EASDomain": "g3",
      "EASServer": "ex2010.mycompany.com",
      "useKCD": "true"
   },
   "dev.mycompany.com": {
      "EASDomain": "dev",
      "AutodiscoverURL":     "https://dev.mycompany.com/autodiscover/autodiscover.xml",
      "skipShortSetup": "true",
   }
}
```

In this example, there is one global parameter: **disableSSLCertificateChecking** . There are also two Domain overrides: **mycompany.com** and **dev.mycompany.com**. The domain override allows us to set parameters specific to that domain.

For the **mycompany.com** domain, we are hardcoding the **EASServer** parameter to a specific EAS server, and KCD is enabled (**useKCD**). In the second domain, **dev.mydomain.com**, Autodiscover (**AutodiscoverURL**) is used, the EAS short form is skipped (**skipShortSetup**).

Default Values for Empty Settings

Settings can be empty; if a setting is not specified (entered into Good Control) or its value is invalid, client default values are assumed.

Format

Configuration settings must be specified in valid JavaScript Object Notation (JSON) according to the standard protocol defined in RFC-4627.

Global Level

The Global level container is a JSON Object signified by curly brackets; i.e., **{}**.

```
{}
```

Members may include:

- Any number of optional **Settings** – when placed in the Global Level container these are treated as "Global" and will apply in the absence of a domain override setting
- Any number of optional **Domain Override** objects.

Domain Override

An object inside the top level object that contains any number of domain specific "override" settings is called a **Domain Override**. The name of the object is the host to which override settings will be applied. The value is the object, which can contain any number of settings members.

```
{
   "setting" : "Global Default"
   "domain.com" = { "setting" : "Override" }
}
```

Members:

Any number of optional **Settings** – when placed in the domain container these will only apply to email addresses ending in that domain and will override the Global setting.

Settings

Settings are members of either the global object or a domain object; each being a member value of these objects.

```
"SettingName" : "Setting Value"
```

See Definitions below for a description of function and example values.

Override Values Inheritance

Inheritance precedence adheres to the following rules:

1. All settings can have a scope at either the global level or the domain level.
2. If a setting is present in the client's domain, the setting will be what is set in the domain object.

3. If not present in the domain object, the client will look for the setting choice in the Global Level and use that.
4. If set in neither, the client will apply its out-of-the-box default settings.

Definitions

Definitions of each setting and value type, including working descriptions and examples, are set forth below.

> **Important:** The number of settings and control points will continue to expand as more and more features are added to BlackBerry Work and existing features are enhanced. Coinciding with each BlackBerry Work software version release, be sure to check new postings of this document for updates and revisions.

Value Types

Type	Description	Examples
BOOL	Boolean, True or False, can be JSON standard true, false, strings "true", "false" or numbers 0, 1	"true", "false", true, false, 0, 1
URL	Fully Qualified URL, including scheme	"http://www.myserver.com", "https://secureserver.corp.com"
Time Interval	Time interval in minutes	60, 5, 3600
Unsigned Integer	Positive whole number	1, 200, 443, 8000, 80
Server name	Name of server (non-qualified)	"myserver.com", "bems.mycompany.com"
Protocol	Valid web protocol	"http", "https"
String	Valid string	"TenantIdentifier", "Purple"

Security Settings

Setting	Type	Client Default	Effective	Description
disableSSLCertificateChecking	BOOL	"false"	At provisioning	Disables SSL certificate verification for ActiveSync / EWS server in test and POC environments Setting functions as expected at global level and domain level. If domain level is set different than global level, domain level will override the global level.
useKCD	BOOL	"false"	Immediately	If enabled, Kerberos Constrained Dispatch will be used for login (user won't be able to, or required if configured properly to enter a password for ActiveSync), otherwise NTLM / Basic authentication will be used. Setting functions as expected at global level and domain level. If domain level is set different than global level, domain level will override the global level. If the Exchange Server and Good Control have KCD enabled the behavior of useKCD = false with the iOS client will allow setup to proceed with the KCD provided password when any

Setting	Type	Client Default	Effective	Description
				characters are entered into the Account Setup Password field. See Implementing KCD for BlackBerry Work for additional guidance.
useEASAuthCert	BOOL	"false"	Immediately	If enabled, clients must have individual login certificates (SSL) uploaded in GC. These certificates will be used for login in place of basic credentials (login / password) Android: Setting functions as expected at global level and domain level. If domain level is set different than global level, domain level will override the global level.

BEMS Settings

Setting	Type	Client Default	Effective	Description
serverListReshufflePeriodInMinutes	Time Interval	2880 (2 days)	At provisioning	Frequency that server list (if present) will be reshuffled, for load balancing purposes
serverListQuarentinePeriodInMinutes	Time Interval	iOS - 5 minutes	At provisioning	If a BEMS server is not working, BlackBerry Work will wait this period before retrying

Exchange Settings

Setting	Type	Client Default	Effective	Description	BlackBerry Work Version Required
disableEWS	BOOL	"false"	At provisioning	When set to "true", client will disable all EWS activities including calendar forward and calendar attachment. Only works on the global level, not domain level.	
EASDomain	String	none	At provisioning	Windows NT Domain to try automatically when logging in. If your server uses newer UPN (email@host.com) style login instead of the older (domain\user) style login, this field should be omitted. Setting functions as expected at global level and domain level. If domain level is set different than global level, domain level will	

Setting	Type	Client Default	Effective	Description	BlackBerry Work Version Required
				override the global level.	
EASServer	Server Name	none	At provisioning	Default Exchange Server used to attempt to connect; used in place of AutodiscoverURL	
AutodiscoverURL	URL	none	Immediately	If provided, and attempts to connect to EASServer fail (or no EASServer is provided) will attempt autodiscovery directly to the URL provided. (This is more secure than "Automated Autodiscovery" which relies on guessing the Autodiscover URL based on DNS entries.) Setting functions as expected at global level and domain level. If domain level is set different than global level, domain level will override the global level.	
EASAuthenticationMethods	List (String)	Blank (all allowed)	Immediately	[iOS] If set, list of allowed authentication methods for Exchange ActiveSync. Allowable values are: • Negotiate • Basic • NTLM • ClientCertificate Value should be a JSON array of allowed methods. Example: `["NTLM","Basic"]` disallows Negotiate, and ClientCertificate methods.	2.2.1
EWSAuthenticationMethods	List (String)	Blank (all allowed)	Immediately	[iOS] If set, list of allowed authentication methods for Exchange EWS. Options are "Negotiate," "Basic," "NTLM," and "ClientCertificate." Value should be a JSON array of allowed methods. Example ["NTLM,""Basic"] would disable Negotiate and ClientCertificate methods.	2.2.1
AutodiscoverTimeout	Number	30	Immediately	[iOS] Autodiscover connection timeout in seconds.	2.2.1
UseServerAutodiscover	BOOL	"false"	Immediately	[iOS/Android] When set to "true," client will use the Server Autodiscover API to determine the EAS/EWS endpoint for the user.	2.2.1

Setting	Type	Client Default	Effective	Description	BlackBerry Work Version Required
skipShortSetup	BOOL	"false"	At provisioning	When **true**, takes the user directly to the long setup form, requiring user input of a recognized AD username, password, and domain during device activation. This is a domain setting. Do not use as a global setting.	
EWSServerURL	String	None	At provisioning	EWS Server URL endpoint. (Example: https://mydomain.com/EWS/Exchange.asmx)	
enableIRM	BOOL	"false"	Immediately	Exchange Information Rights Managements for mail. To exercise IRM in this release, add the following line to your JSON settings: "enableIRM": "true",	2.2.1

Client Settings

Setting	Type	Client Default	Effective	Description
syncEmailBodySize	Number	iOS: 20 Android: 8	At provisioning	Size in Kbytes of the partial message body downloaded from server if the user selects the option to download partial message content. (iOS default 20 = 20 Kb / Android default 8 = 8 Kb) Setting this value to 0 will prevent automatic download of email body (preview will still be present, but no data will be downloaded on initial sync, only when user opens an email specifically).

Other Settings

Setting	Effective	Description	BlackBerry Work Version Required
ContactEmail	At provisioning	[Android] Admin setup information - Displays in account setup long form.	
ContactPhone	At provisioning	[Android] Admin setup information - Displays in account setup long form.	
SendFeedbackEmail	Immediate	Sends client feedback email to "blackberryadmin@acme.com." Add multiple recipients as needed.	2.2.3
phishingReportEmail	Immediate	Enables users to report emails considered as phishing. The reported emails are being forwarded to the email address provided in this field then moved to Trash folder. Example: "phishingReportemail"."*forwarding_address*"	2.3.0

Appendix D – GFE to BlackBerry Work Deployment and Migration

For existing BlackBerry for Enterprise (GFE) deployments, please note the following considerations before deploying BlackBerry Work. See also *GFE Migration to BlackBerry Work Transition Guide*.

GFE Material Parity

In this first release (1.1) of the BlackBerry Work client with BEMS (1.1), complete material parity with GFE will be deferred to subsequent releases. If the capabilities and compatibilities listed below are required in your environment, then a full transition to the BlackBerry Work client and BEMS from GFE is currently not possible. Consequently, until full material parity with GFE is achieved, a POC or limited deployment of the BlackBerry Work client with BEMS is recommended.

BEMS-BlackBerry Work/GFE Feature Disparity

The main potential disparities to consider include:

Mobile Device Management (MDM)

In version 1.1 of BlackBerry Work, some device specific MDM policies available in GFE are not supported. However, because the BlackBerry Work client is built on the BlackBerry Dynamics platform, it is FIPS-certified with AES 256 encryption. Likewise, features such as jail break detection, remote wipe, offline wipe, OS verification, etc., are all available in BlackBerry Work v1.1.

Domino Mail

Domino mail is not currently supported by the BlackBerry Work client.

S/MIME

S/MIME, however, is now supported by BlackBerry Work.

Appendix E – File Types Supported by BlackBerry Work

The following file types/extensions are currently supported by the Docs service and as mail attachments (some require third-party applications to view):

- .goodsharefile,
- .doc, Docx
- wordprocessingml.document,
- powerpoint.ppt, PPTx
- excel.xls, XLSX
- spreadsheetml.sheet,
- adobe.pdf,
- apple.rtfd,
- apple.webarchive,
- .image,
- .jpeg,
- .tiff,
- .apple.pict,
- .compuserve.gif,
- .png,
- .quicktime-image,
- .bmp,
- .camera-raw-image,
- .svg-image,
- .text,
- .plain-text,
- .utf8-plain-text,
- .utf16-plain-text,
- .rtf,
- .html,
- .xml,
- .xhtml,
- .htm,
- .data,
- .content
- .zip

- Media Files (iOS only)
  - .3gp
  - .mp3
  - .mp4
  - .m4a
  - .m4v
  - .wav
  - .caf
  - .aac
  - .adts
  - .aif
  - .aiff
  - .aifc
  - .au
  - .snd
  - .sd2
  - .mov

Appendix F – Exchange Active Sync (EAS) Search Limits

ActiveSync Search Command

Mailbox (email search): 100 limit. Search will return the top 100 entries. It also returns the total match. You can then refine your filter to get the relevant data into the top 100 entries.

GAL (to find contacts/recipients in GAL): up to 100 entries.

Compose Email Recipient Search

Less than 3 chars: Combine data from Local Contacts DB + data from **GCSCRecipient** table in DB.

More than 3 chars: Use GAL Search. (see above)

Appendix G – Whitelisting Native and Third-Party Apps for "Open In"

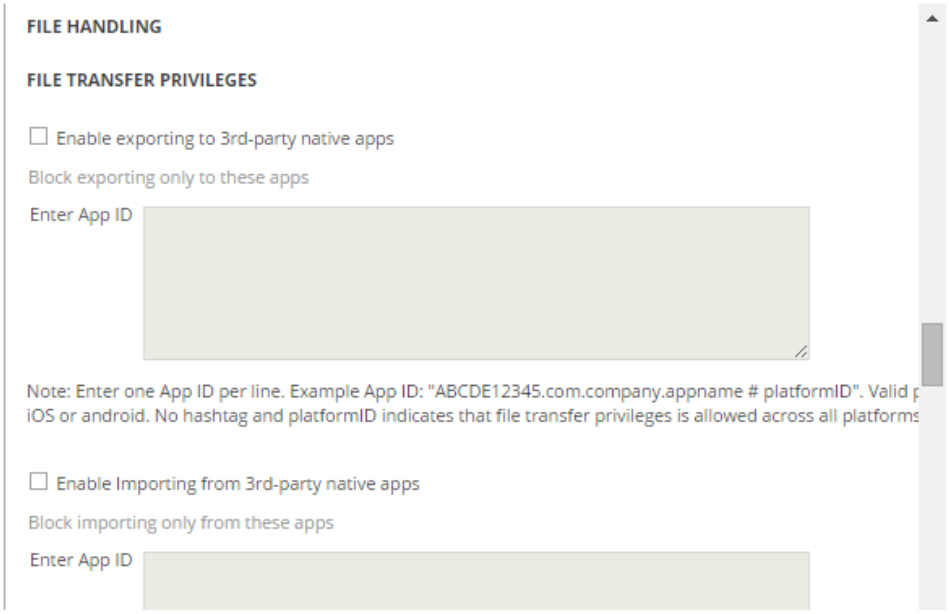
Application whitelisting is an administration practice used to prevent unauthorized programs from sharing data in the BlackBerry secure container on user devices.. Its primary purpose is to protect your devices and networks from harmful or unreliable applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Put another way, the "whitelist" is a collection of apps that have been approved by IT administration for importing data to or exporting data from the BlackBerry secure container on provisioned devices. This is done using an **Application Policy** in Good Control, in which you can also explicitly block file transfer privileges for a "blacklist" of third-party apps.

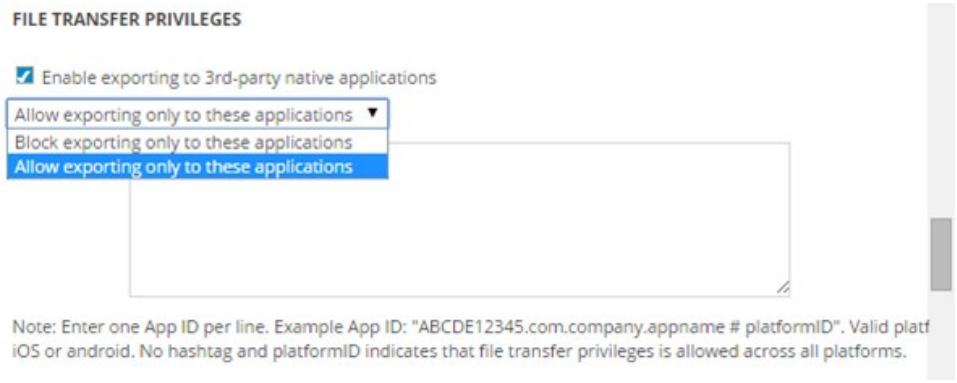
The procedure described here applies to all apps, not just the Voltage SecureMail example. Consequently, care should be exercised in determining import versus export whitelisting/blacklisting. You will need the respective App IDs for each iOS and Android version of the application you want to whitelist or blacklist.

To whitelist a third-party or native app for file export:

1. Login to Good Control.
2. Under **POLICIES**, click **Policy Sets**.
3. Click on the policy set you want to modify, then open the **APP POLICIES** tab.
4. Scroll down to **BlackBerry Work** and click it, then open the **Interoperability** tab.
5. Scroll down to the **FILE HANDLING** section; then, under **FILE TRANSFER PRIVILEGES**, check **Enable exporting to 3rd-party native applications**.

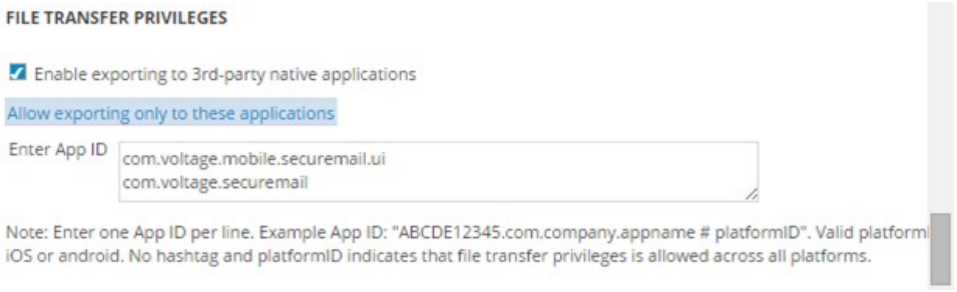


6. Select **Allow exporting only to these applications** from the drop-down list.



7. In the **Enter App ID** texbox, enter one App ID per line. As noted, omitting the hash tag and platformID (iOS or android) allows file transfer privileges across all platforms.

   In the example, the first App ID for Voltage SecureMail (**com.voltage.mobile.securemail.ui**) is for the Android app; the second, **com.voltage.securemail**, is for iOS. Because the App ID for each respective platform is different, no hash tag or platformID is needed .



8. Click **Update** to save your changes.

With the policy in place, your iOS and Android users who have the Voltage Secure Mail app installed on their devices will be able to read **message_ZDN.html** attachments from their BlackBerry Work emails using the Open In (iOS) feature or Share (Android) feature, respectively.

Appendix H – Changing Mail Message/Attachment Limits in Exchange

The message size limit for an Exchange mailbox stems from the **Maximum send size** setting that is configured in the **Transport Settings Properties** dialog box by the Exchange administrator.

Configuring Max Message Size

To set/change the maximum size of a message that is sent through an Exchange Server account:

1. Start the Exchange Management Console (EMC).
2. Under **Organization Configuration**, click **Hub Transport**.
3. On the **Global Settings** tab, click **Transport Settings**.
4. In the **Transport Settings** section of the **Actions** pane, click **Properties**.
5. Open the **General** tab in the **Transport Settings Properties** dialog box and configure the value for **Maximum send size (KB)**.
6. Click **OK**.

> **Note:** Because the Exchange server has a cache for various settings, this change will not take effect immediately. You may have to wait several hours before this change is recognized.

Configuring Attachment Size Limit

The only way to set size limits in Exchange exclusively for attachments is to use a hub transport rule, which will detect and block messages if their attachments are over a specified size threshold.

To set up the rule you can use the following PowerShell script:

```
New-TransportRule -Name LargeAttach -AttachmentSizeOver <limit>MB -RejectMessageReasonText "Message attachment size over <limit>MB - email rejected."
```

For example:

```
New-TransportRule -Name LargeAttach -AttachmentSizeOver 10MB -RejectMessageReasonText "Message attachment size over 10MB - email rejected."
```

The command creates a rule (**LargeAttach**) triggered by any email with attachments larger than 10MB. You can, of course, increase or decrease this limit. The rule then stops the message from delivery and sends back a notification about that fact to the original sender.

Resolving EAS Max Request Length Exceeded Errors

This issue is most commonly caused by the default IIS configuration on Exchange CAS servers that limits incoming messages to between 4–10MB in size (depending on version), regardless of the limits set elsewhere in the Exchange organizational or user configurations. You will know this is the problem if you see the following event frequently in your Exchange CAS Application event logs:

```
EVENT LOG Application
EVENT TYPE Warning
SOURCE MSExchange ActiveSync
EVENT ID 1008

MESSAGE
An exception occurred and was handled by Exchange ActiveSync. This may have been caused by an outdated or
corrupted Exchange ActiveSync device partnership. This can occur if a user tries to modify the same item from
multiple computers. If this is the case, Exchange ActiveSync will re-create the partnership with the device.
Items will be updated at the next synchronization.

URL=/Microsoft-Server-
ActiveSync/default.eas?Cmd=SendMail&DeviceId=393930303031313834343383037&DeviceType=iPhone4S&SaveInSent=T
--- Exception start ---
Exception type: System.Web.HttpException
Exception message: Maximum request length exceeded.
Exception level: 0
Exception stack trace: at System.Web.HttpRequest.GetEntireRawContent()
at System.Web.HttpRequest.get_InputStream()
at Microsoft.Exchange.AirSync.Command.get_InputStream()
at Microsoft.Exchange.AirSync.Command.WorkerThread()
--- Exception end ---.
on message: Maximum request length exceeded.
Exception level: 0
Exception stack trace: at System.Web.HttpRequest.GetEntireRawContent()
at System.Web.HttpRequest.get_InputStream()
at Microsoft.Exchange.AirSync.Command.get_InputStream()
at Microsoft.Exchange.AirSync.Command.WorkerThread()
--- Exception end ---
```

Not only does this cause a poor end-user experience, it can also cause very high data usage that can be costly. Fortunately, there is a reasonably easy solution.

To change the default IIS configuration for incoming message size:

1. On your CAS server, navigate to your Exchange program folders; i.e., on Exchange 2010 in **C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Sync**.
2. Make a copy of the existing **web.config** file as a backup.
3. Open the **web.config** file and look for the entry: **<httpRuntime maxRequestLength="10240"/>**
4. Change the entry to a much larger number. We recommend 50MB, or an entry of **51200**, in order that this limit is never reached.
5. Save the file.

Normally **web.config** changes are picked up automatically so you don't need to restart IIS, but you can run **iisreset /noforce /timeout:200** for good measure.

This allows for large attachments to still make it through from the device, and then hit your actual Exchange-based attachment limits where the user will get a normal rejection message instead of just getting stuck on the device and chewing up all your data.

Appendix I – BlackBerry Work Badge Count

BlackBerry Work for iOS uses the Apple Push Notification Service (APNS) to wake up apps or update the badge count displayed as a number on the app icon, also known as the "badge." Users can configure the badge count to indicate either the number of unread emails or the number of new emails, as explained in the BlackBerry Work Client User Guide for iOS Devices under "Changing Your BlackBerry Work Application Settings."

This appendix focuses on badge count behavior and optimization from an administration perspective.

New Mail

The **New Mail Badge Count** setting—which is also the badge count default setting—reflects the number of emails received since the user last closed the app. However, the badge count value will not decrement if the user checks their email from a desktop or laptop workstation.

Unread Mail

In BlackBerry Work **Settings**, each user has the option of changing the badge count preference to **Unread Mail**. Under this option, designed to optimize battery life, the badge count will reflect the number of unopened/unread emails within the chosen synchronization time period as an indicator of outstanding messages needing attention.

Optimization and Limitations

Technical optimizations for best battery performance and Apple OS limitations pertinent to the Unread Mail badge setting include:

1. The badge count for the Unread Mail preference is updated even if the app is not running in the background. This is achieved by requesting BlackBerry Enterprise Mobility Server (BEMS) to send an Apple push notification using APNS. Apple does not guarantee that all push notifications will wake up the app or update the badge count.
2. BEMS throttles push notifications to optimize battery performance on mobile devices. Each push notification consumes some battery power when lighting up the “Home & Lock Screen.” Push notifications for new emails are sent no more frequently than once a minute and for updates. Silent push notifications for update or delete operations performed on desktop or other devices are sent no more than once every 15 minutes. If the user is triaging emails on the desktop but does not receive a new email, the unread count will be updated when the next APNS is received, generally within 15 minutes. The badge for unread mail, however, does not decrement if the user checks email on their desktop or laptop.
3. The unread count is shown only for emails that are actionable within the sync window. This ensures that the user can see the same count in the Unread smart folder. The app provides the last known unread count to BEMS when going into background and bEMS increments it using push notifications.

   Note: If the app is unable to reset the last known unread count when going into background (due to network connectivity issues, server connectivity issues, user is offline, or app crash), the count will not be accurate until the

next successful BEMS connection. Additionally, if the client has not fully completed its sync operation, the unread badge count will be inaccurate.

Administration Policy

Based on the OS limitations and battery optimizations cited above, a company may choose to only allow **New Mail** badge counts, similar to those supported by Good for Enterprise. As of v1.5.3, BlackBerry Work allows companies to configure this so an end user will only see the new mail badge count option.

Appendix J – BlackBerry Tasks and BlackBerry Notes

Introduction

BlackBerry Tasks and BlackBerry Notes are enterprise PIM applications that enable users to create, open, and manage tasks and notes synchronized with Microsoft Exchange service.

The BlackBerry Tasks and BlackBerry Notes apps are built for use on the BlackBerry Dynamics Secure Mobility Platform and will not operate without the necessary back-end software. Users will need their Outlook credentials to use the app.

Note: BlackBerry Tasks and Notes do not use Microsoft Exchange ActiveSync like BlackBerry Work does, but leverage Microsoft Exchange Web Services. This is a different end point on the Microsoft Exchange CAS servers and therefore may have different authentication configurations (e.g., Certificate Based Authentication for EAS, but Username/Password for EWS).

Setup

To prepare your environment for BlackBerry Tasks and Notes, configure the BlackBerry Tasks and Notes apps in Good Control. Configuration consists of completing setup tasks using similar instructions as those provided for the BlackBerry Work app:

- Add the BEMS host servers to BlackBerry Tasks and Notes to allow assisted AutoDiscover; same steps as for BlackBerry Work - Adding BEMS to the BlackBerry Application Server List

  BEMS is only required if you are using Configuring Exchange Autodiscover .
- Entitle BlackBerry Tasks and Notes to Users or Groups; same steps as for BlackBerry Work - Adding Applications and Users in Good Control
- Configure BlackBerry Tasks for Notifications (Tasks only), Configuration options, and Exchange Server settings - Setting BlackBerry Tasks and Notes Application Policies
- Review Authentication Delegation options. It is recommended to set BlackBerry Work as the Authentication Delegate - Authentication Delegation

Setting BlackBerry Tasks and Notes Application Policies

For an overview of GC dashboard setup, refer to Configuring the BlackBerry Work App in Good Control . The information found there applies also to BlackBerry Tasks and Notes except where outlined below.

Policy sets contain rules that govern the security of GD applications and rules specific to the devices and OS versions configured in Good Control.

To set an application-specific policy for BlackBerry Tasks or Notes:

- In the Good Control console navigator (left-hand panel) click Policy Sets, select a policy to clone and/or modify by clicking it, then click the APPS tab and expand the APP SPECIFIC POLICIES list.
- Scroll down to select BlackBerry Tasks or BlackBerry Notes from the list by clicking it.

Notification Policy (Tasks Only)

On the Notifications tab, choose to turn off Tasks notifications on the user's device, or to display a generic notification, or to display the title of of the task in the notification.

Configuration Settings

On the Configuration Settings tab, configure the available security and BEMS settings as desired.

Security settings:

Enable security settings by clicking the appropriate checkboxes.

- Disable SSL Certificate Checking - Disables SSL certificate verification for Microsoft Exchange Web Service servers in test and POC environments. Effective at provisioning.
- Permit the use of Kereros Constrained Delegation - If enabled, Kerberos Constrained Delegation will be used for login (user won't be able to, or required if configured properly to enter a password for ActiveSync); if not enabled, NTLM/Basic authentication will be used. Effective at provisioning.

  If the Exchange Server and Good Control have KCD enabled the behavior of the checkbox with the iOS client will allow setup to proceed with the KCD provided password when any characters are entered into the Account Setup Password field.

  See Implementing KCD for BlackBerry Work for additional guidance.
- Clients must have individual login certificates (SSL) uploaded in the GC - These certificates will be used for login in place of basic credentials (login/password). Effective at provisioning. This is a requirement if Certificate Based Authentication is required for Microsoft Exchange Web Services.

Embedded Hyperlink Support:

- Do not allow user to open hyperlinks
- Only allow secure browser
- Prefer secure browser but allow device browser

Enterprise Mobility Server:

- Reshuffle period - Frequency that Enterprise Mobility Server (BEMS) server list (if present) will be reshuffled, for load balancing purposes. The default is 10 minutes. Effective at provisioning.
- Server list - If a BEMS server is not working, BlackBerry Tasks will wait this period before retrying. The default is 10 minutes. Effective at provisioning.

Exchange Settings

On the Exchange Settings tab:

In the EXCHANGE WEB SERVICES AUTHENTICATION METHODS (IOS ONLY) section:

Use following Authentication Methods:

- Negotiate
- NTLM
- Basic

Select allowed authentication method from Exchange Web Services setting. If only certain authentication methods are supported from Exchange, set those values to minimize the user setup time. (E.g. if EWS IIS Auth Setting is set to allow only NTLM, then select only NTLM above for an optimal setup experience.) If none are selected above, default Exchange setting will be used. Do not check any of these options if using client-based authentication.

In the MICROSOFT EXCHANGE SETTINGS section, specify the Microsoft Exchange domain and server name:

The Exchange domain is the Windows NT Domain to try automatically when logging in. If your server uses newer UPN (email@host.com) style login instead of the older (domain\user) style login, leave this field blank.

In the Exchange Server field, enter the Fully Qualified Domain Name of the server or CAS Array or Load Balancer responsible for providing Microsoft Exchange Web Services. if you leave this field blank, BlackBerry Tasks will leverage Assisted AutoDiscover via BEMS if BEMS is configured and if BEMS is listed in the Application Server List for BlackBerry Tasks. Note: Enter *only* the Fully Qualified Domain name of the Exchange server. Do not include a protocol prefix such as https:// or a URI suffix.

In the EXCHANGE WEB SERVICES USER NAME FORMATS (IOS ONLY) section:

Select the User Name Formats to be used to authenticate with Exchange Web Services. If only certain User Name Formats are supported from Exchange, set those values to minimize the user setup time. (E.g. if EWS Auth Settings are set to allow only SMTP but not UPN, then de-select UPN in the app setting.) If none are selected, authentication with all User Name Formats will be attempted.

Choices are UPN, Domain/UserId, and SMTP.

In the EXCHANGE TLS CERTIFICATE SETTINGS section:

Specify the User Credential Profile Name for the TLS certificate to be used for Exchange connection. Enter the User Credential Profie Name exactly as entered in UEM Console.

In the OFFICE 365 SETTINGS (BETA) section:

Click checkbox for "Use Office 365 Settings" to use Office 365 Setup Configuration for Work mailbox account setup.

Click checkbox for "Use Office 365 Modern Authentication" to use Office 365 Modern Authentication when logging into Work mailbox account.

Enter an Office 365 Sign On URL. If left blank, Work setup will try https://login.microsoftonline.com during an initial setup.

Enter Office 365 Tenant ID. If left blank, Work will use "common" during an initial setup.

Enter the Application ID registered in your Azure Portal– Using ADAL for Authentication

App Settings

On the App Settings tab, there is a setting to allow users to perform app diagnostics. The default is Checkbox Enabled.

Appendix K – Exchange Classifications and Caveats

Users can select Exchange classification and caveat settings that you make available to them by policy, by editing the xml file on the Classification tab as described in Step 6 in Setting BlackBerry Work Application Policies

Example:

```
<emailClassificationMarks>
  < options>
    <classifications>ON</classifications>
    <caveats>OFF</caveats>
    <classificationDefault>INTERNAL</classificationDefault>
    <caveatDefault>NO FORWARD</caveatDefault>
  </options>
  <classifications>
    <classification>
      <select>INTERNAL</select>
      <subject>(INTERNAL)</subject>
      <topBody>Classification:  INTERNAL</topBody>
      <bottomBody>Classification:  INTERNAL</bottomBody>
      <caveatOptions>
        <caveatOption>
          <caveatSelect>NO  FORWARD</caveatSelect>
          <state>ON</state>
        </caveatOption>
        <caveatOption>
          <caveatSelect>NO  REPLY</caveatSelect>
          <state>OFF</state>
        </caveatOption>
      </caveatOptions>
    </classification>
    <classification>
      <select>CONFIDENTIAL</select>
```

```
            <subject>[CONFIDENTIAL]</subject>
            <topBody>Classification: Confidential</topBody>
            <caveatOptions>
                <caveatOption>
                    <caveatSelect>NO REPLY ALL</caveatSelect>
                    <state>OFF</state>
                </caveatOption>
            </caveatOptions>
        </classification>
    </classifications>
    <caveats>
        <caveat>
            <select>NO  FORWARD</select>
            <subject>(DO  NOT  FORWARD)</subject>
            <topBody>Caveat: DO NOT FORWARD</topBody>
            <bottomBody>Caveat: DO NOT FORWARD</bottomBody>
        </caveat>
        <caveat>
            <select>NO REPLY</select>
            <subject>(DO NOT REPLY) </subject>
        </caveat>
        <caveat>
            <select>NO REPLY ALL</select>
            <subject>(DO NOT REPLY ALL)</subject>
        </caveat>
    </caveats>
</emailClassificationMarks>
```

Notes:

- Only one classification and caveat can be specified by the user in an email. Only one classification and caveat can be specified by the admin in XML for the default classification and caveat.

- A Classification can contain multiple caveats.
- If a default classification and caveat are defined by the admin in XML, the user will see this classification and caveat as the initial choices when composing an email. Tapping on the Classifiction and Caveat pulldown menus will display a list of the other classifications and general caveats defined in the file and available to choose for an email. Optional caveats are not available from the general caveat list.
- If a default classification is not defined in XML (left empty), the user has the option of defining a default classification and caveat using BlackBerry Work Mail Settings on their device, choosing from the lists of classifications and general caveats. Optional caveats are not available in this list. If the admin defines defaults classifcation and caveat, settings to do so are not also available to users on their device.
- Optional caveats, which are added to specific classifications, are not displayed in the user's general caveat list.
- Changing the name of a classification or caveat in XML does not otherwise change its behavior with respect to display and use.
- If Classification A contains optional caveats a, b, and c, the user, when choosing that classification from the list, with see only the associated caveats in the caveat list; that is, the Caveat dropdown will contain only a, b, and c. If the user changes the classification to B, the caveat list will display only Bs assoicated caveats. However, if the admin specifies Classification A as the default, when the user switches to Classification B, the caveat dropdown choices remain those of Classification A.

Appendix L – Using ADAL for Authentication

The Azure Active Directory Authentication Library (ADAL) enables applications to easily authenticate users to cloud or on-premisess Active Directory (AD),

To use ADAL as the authentication method for BlackBerry Work, Tasks, or Notes:

- Set up ADAL according to the Microsoft instructions. (Refer to the links below for related information.)
- Set up GC as described in the following section.
- Obtain an Azure App ID as described below.

Setting up GC

To use ADAL with BlackBerry Work, Tasks, or Notes, enable the following policy settings in GC:

1. In GC, go to Policy Sets -> Good Default Policy -> Apps ->App Specific Policies -> BlackBerry Work (or Tasks or Notes) -> Exchange Settings
2. Check "Use Office 365 Settings." This will use the Office 365 Setup Configuration for the Work mailbox account setup.
3. Check "Use Office 365 Modern Authentication." This will use Office 365 Modern Authentication when logging into the Work mailbox account.
4. Enter an Office 365 Sign On URL. If let blank, Work setup will try login.microsoftonline.com during an initial setup. (Optional)
5. Enter an Office 365 Tenant ID. If left blank, Work will use "common" during an initial setup. (Optional)
6. Enter an Azure App ID. Refer to the following section for information on obtaining this ID.

Obtaining an Azure App ID

1. Log on to portal.azure.com.
2. Select "Azure Active Directory…"
3. Select "App Registrations."
4. Ciick on "New application registration."
5. Enter a name for the application.
6. Set the application type to "Native."
7. Set redirect URL to "com.blackberry.work://connect/o365/redirect."
8. Click on Create.
9. Select the application name that is created.
10. Click on Required permissions.
11. Click on Add.

12. Select “Select an API” and select “Office 365 Exchange Online (Microsoft Exchange).
13. Set the permission for Office 365.
14. Add another permission for “Microsoft Graph” and apply the two permissions Application Permissions and Delegated Permissions.

Related Links

Microsoft Exchange Server Deployment Assistant

The Exchange Server Deployment Assistant is a web-based tool that asks you a few questions about your current environment and then generates a custom step-by-step checklist that will help you deploy different versions of Exchange Server for different types of scenarios.

https://technet.microsoft.com/en-us/office/dn756393.aspx

Hybrid Deployment Prerequisites

https://technet.microsoft.com/en-us/library/hh534377(v=exchg.150).aspx

Hybrid Configuration Wizard

https://technet.microsoft.com/en-us/library/hh529921(v=exchg.150).aspx

MS Video

Step-By-Step: Configuring a Hybrid Office 365 Deployment via Hybrid Deployment Wizard

https://blogs.technet.microsoft.com/canitpro/2016/05/09/step-by-step-configuring-a-hybrid-office-365-deployment- via-hybrid-deployment-wizard

“Office 365 Exchange Hybrid Deployments Busting The Autodiscover Myth”

https://blogs.technet.microsoft.com/rmilne/2016/07/14/office-365-exchange-hybrid-deployments-busting-the-autodiscover-myth

Exchange Q & A: Handling Hybrid Environments

https://technet.microsoft.com/en-us/library/dn249970.aspx

“Do I really need to use ADFS in O365 / Azure AD?”l

https://blogs.technet.microsoft.com/pie/2017/02/06/do-i-really-need-adfs

Note that attention is required for IDAM deployment, specifically ADFS deployment.

Plan Your ADFS Deployment

https://technet.microsoft.com/en-us/library/dn151324.aspx

Office 365 SSO: A Simplified Installation Guide

https://technet.microsoft.com/en-us/library/jj631606.aspx

Hybrid Identity Required Ports and Protocols

The following document is a technical reference on the required ports and protocols for implementing a hybrid identity solution.

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-ports

Connectivity Prerequisites

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-prerequisites