Good Mobile Access
(Secure Browser) Guide

A Component of Good for Enterprise
Legal Notice

This document, as well as all accompanying documents for this product, is published by Good Technology ("Good"). Good may have patents or pending patent applications, trademarks, copyrights, and other intellectual property rights covering the subject matter in these documents. The furnishing of this, or any other document, does not in any way imply any license to these or other intellectual properties, except as expressly provided in written license agreements with Good. This document is for the use of licensed or authorized users only. No part of this document may be used, sold, reproduced, stored in a database or retrieval system or transmitted in any form or by any means, electronic or physical, for any purpose, other than the purchaser’s authorized use without the express written permission of Good. Any unauthorized copying, distribution or disclosure of information is a violation of copyright laws.

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of Good. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those written agreements.

The documentation provided is subject to change at Good’s sole discretion without notice. It is your responsibility to utilize the most current documentation available. Good assumes no duty to update you, and therefore Good recommends that you check frequently for new versions. This documentation is provided “as is” and Good assumes no liability for the accuracy or completeness of the content. The content of this document may contain information regarding Good’s future plans, including roadmaps and feature sets not yet available. It is stressed that this information is non-binding and Good creates no contractual obligation to deliver the features and functionality described herein, and expressly disclaims all theories of contract, detrimental reliance and/or promissory estoppel or similar theories.

Patents, Legal Information & Trademarks

©Copyright 2013. All rights reserved. Good Technology, Good, the Good logo, Good for Enterprise, Good For You, and Good Mobile Messaging, are either trademarks or registered trademarks of Good. All third-party trademarks, trade names, or service marks may be claimed as the property of their respective owners and are used only to refer to the goods or services identified by those third-party marks. Good’s technology is protected by U.S. Patents 6,085,192; 5,968,131; 6,023,708; 5,961,590; 6,131,116; 6,151,606; 6,233,341; 6,131,096; 6,708,221 and 6,766,454 along with numerous other U.S. and foreign patents and applications pending.

Good Technology, Inc.
430 N. Mary Avenue, Suite 200
Sunnyvale, CA 94085

http://www.good.com

Be Good. Be Safe.

Please do not use while driving or engaged in any other activity that requires your full attention.
# Table of Contents

Overview  2  

Preparation  4  
  Using Kerberos Authentication  4  

Enabling Secure Browser  7  
  Using a Proxy with GMA Secure Browser  9  

Usability  14  
  Good Mobile Access within Good For Enterprise version 2.1 iOS/Android Secure Browser Feature Comparison  15  
  SSL Server Certificate Validation  17  
  Client Certificate-based Authentication Support  18  
  Disabling Redirection To Native Browser  19  
  Saving a Document to the Repository and Opening the Document in Another Application  20  

Troubleshooting  20  

Frequently Asked Questions  25  
  General  25  
  Supported Technologies  26  
  Best Practices  29  
  Usage Scenarios  29  

Document Revision List  31
Good Mobile Access (Secure Browser)

Good Mobile Access (Secure Browser) is a Good Messaging plugin that provides a browser on supported devices for use with your corporate intranet. The browser is integrated to the Good Mobile Messaging Client on the device and provides seamless access to intranet sites without need for VPN.

Good Mobile Access (Secure Browser) uses Console policies to determine whether a web page should be loaded on the user’s device or redirected to the native browser. The secure-browser policy lists all the intranet domains, sub-domains, and embedded internet domains that you as administrator want to make available on the mobile device.

The secure browser provides a browser history, which can be cleared. Naming and editing bookmarks is supported. The browser supports pinch and zoom, and landscape mode. No special training is required.

Secure Browser supports HTML4. For a list of Secure Browser features that will work with HTML5, refer to the separate document “Support for HTML5 and CSS3.”
Overview

Good Mobile Access (Secure Browser) provides browsing-only functionality for supported devices. It does not provide connectivity for other applications to your intranet. It utilizes the secure container for browsing, thus storing all the data in encrypted format. The browser is included with Good Mobile Messaging Server and does not require additional server installation. Browser access is at the HTTP level (Application/Proxy layer) rather than the IP packet level (Network Layer). This ensures secure and separate corporate data:

• Integration with the Good for Enterprise iPhone app
• Encryption of browser cache, bookmarks, history and downloaded files inside the enterprise container
• End-to-end encryption of data over-the-air
• No outbound firewall holes
• Application password policies

This graphic illustrates the Client communication flow:

• The user enters a URL in the secure browser.
• The Client issues an HTTP proxy connection over GMM server.
The browser supports an HTTPS connection end-to-end from Client to webserver.

- GMM Server resolves the host name of the requested webserver, checks the host names against the domain list defined by the Secure Browser policy in Good Mobile Control.
- Once the HTTP connection is established, the client performs an HTTP transaction (POST/GET). Good Messaging server will simply pass the data between the webserver and the Client as the session requires.

Notes on the secure transport:

- Over-the-air transmissions are encrypted from the device to the Good Messaging Server using AES 192 Bit Encryption.
- Good Messaging Server establishes a TCP connection to the web server based on the URL being requested by the secure browser.
- Good Messaging server relays data between the web server and the secure browser on the mobile device.
  - Data exchanged between the secure browser and web server is encrypted using HTTPS.
  - Good Messaging Server does not store or analyze any of the data between the secure browser and the web server.
  - Access restrictions are applied based on the administrative policies defined in Good Mobile Control.
Preparation

Before setting up secure browsers for users, confirm the following:

- Good Messaging Server should be able to directly connect to requested host.
- Good Messaging Server should be able to resolve the host name to IP address through DNS lookup.
- Good Messaging Server should be able to directly connect to the resolved IP address and requested port number.

In addition:

- Secure browser requires the Good iOS Client 1.8.2 or higher, or Good Android Client 1.8.2 or higher. No other iPhone or iPad preparation is required. For Android, a WebKit download from the Android Market is required; the first time the user runs Secure Browser, it will lead the user through WebKit installation. Android 2.2, 2.3, and 4.0 devices are supported.
- NTLM v2 (only), and HTTP basic and digest authentication are supported.
- For connection to a host through a proxy server, refer to “Using a Proxy with GMA Secure Browser” on page 9.
- Network problems such as router bottlenecks and inefficient firewalls can manifest themselves in poor browser performance. Some customers have reported that for their networks, changing their router setting from 100MB half-duplex to 1GB full-duplex and deleting old access lists from their firewall improved browser performance.

You can set up a home page for the browsers. You’ll specify it when setting secure-browser policies. The page can serve as a launching point to all your internal web-based resource, streamlining intranet access and making all its resources easily available to your users.

Using Kerberos Authentication

The domain controller (DC) for the Key Distribution Center (KDC) server and services (which the GMA clients communicate with)
needs to have at least one of the following common encryption types to work properly. You do not need to disable Single DES encryption on the KDC server and in service accounts, but you do need to ensure that they are not configured to use only Single DES encryption. In such a case, KDC will not generate a ticket for the GMA client, because it will not have a suitable key to do so. Refer to the following for details: http://support.microsoft.com/kb/977321.

**Secure Browser Supported Encryption Types**

Weak encryption such as Single DES is not supported.

- des3-cbc-sha1
- des3-hmac-sha1
- des3-cbc-sha1-kd
  Triple DES cbc mode with HMAC/sha1

- aes256-cts-hmac-sha1-96
- aes256-cts
  AES-256 CTS mode with 96-bit SHA-1 HMAC

- aes128-cts-hmac-sha1-96
- aes128-cts
  AES-128 CTS mode with 96-bit SHA-1 HMAC

- arcfour-hmac
- rc4-hmac
- arcfour-hmac-md5
  RC4 with HMAC/MD5

- des3
  The triple DES family: des3-cbc-sha1

- aes
  The AES family: aes256-cts-hmac-sha1-96 and aes128-cts-hmac-sha1-96
The Windows KDC server listens by default on port 88 for UDP/TCP, which is suitable for use with GMA. The GMA client connects to KDC server using TCP and according to RFC 4120, KDC accepts TCP requests. If the KDC server listens on a TCP port, communication should work properly. There is no need to make changes on the DC/KDC because all the connections are initiated from the Client and the client whether the connection will use TCP or UDP.

Good testing was performed with KDC installed on Windows Server 2008 R2. No additional changes were made to AD.

**Default Location for Kerberos Configuration File**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows®</td>
<td>c:\winnt\krb5.ini</td>
</tr>
<tr>
<td>Linux®</td>
<td>/etc/krb5.conf</td>
</tr>
<tr>
<td>Other UNIX-based</td>
<td>/etc/krb5/krb5.conf</td>
</tr>
<tr>
<td>z/OS®</td>
<td>/etc/krb5/krb5.conf</td>
</tr>
</tbody>
</table>
Enabling Secure Browser

To enable Secure Browser for users via a policy and to set policies for intranet browser user:

1. Display the Good Mobile Access (Secure Browser) policies page by clicking on its link in the Plugins portion of the left column of the Policies tab.

2. Click the “Enable access to the intranet” checkbox to turn on the browser feature for supported handhelds using this policy (and to display the full screen above).

   **Note:** Although the policy page uses the word “intranet,” enabling access also allows you to specify accessible internet domains for the secure browser.

3. If desired, supply a homepage address for the homepage to be displayed when the Good secure browser is invoked. If no address is specified, the browser opens on a blank page.

4. Enter the specific intranet or internet domains that the browser can access. No other public domains will be allowed. That is, this
list is used as an “allow” list for public IPs: allow hosts with public IPs whose domain suffix matches an entry in this list.

Note: Non-fully qualified domain names (NFQD) are supported, with the exception of names such as .com, .net, .gov, and .edu. With Good Mobile Control 2.3.0, an “Allow non-fully qualified domain” policy is available, to enable or disable.

To enter the domains, click the Edit button.

Type in the domains that you will allow, separated by commas. These can be intranet or internet domains. If an intranet domain includes embedded internet domains, such as in links to the internet on a page or pictures that are referenced from the internet, you’ll want to include those internet domains in this list (see Troubleshooting below).

Wildcards are not supported. However, entering “acme.com” will allow any URLs ending with that string (e.g., “test.acme.com” will be allowed).

Note that if a user enters a non-fully qualified domain name such as http://info, the browser will connect to it by bypassing the domain suffix list that you have entered above.
DNS settings on the Good Messaging Server are used to resolve host names. The Server does not contact DNS providers for the domains you enter in your allowed list, to resolve host names.

**Popups:** Popups are enabled in the browser by adding the following to the allowed domains:

```
15popupflag.gmm.good
```

5. Use the checkboxes to enable:

- Redirect domains not listed above to native browser (enabled by default)
- Allow non-fully qualified host domains (enabled by default)
- Allow user to accept unsigned or expired certificates (enabled by default) (iOS only)
- Allow user to persist enterprise credentials in Good secure container for website and web proxy access (disabled by default)

6. If you will be using Kerberos authentication, click the Kerberos checkbox to enable it. Browse to your Kerberos authentication file and select it. The file will be downloaded to those iOS devices using the policy.

7. If you will be using proxy servers, enter the IP Addresses for the HTTP and HTTPS servers. (Use the Good Mobile Access Secure Browser tab on the Console Settings tab.) If any IP prefixes/domains are to bypass the proxy servers, enter the prefixes and domains, separated by commas, in the field provided, one pair per line. Refer to “Using a Proxy with GMA Secure Browser” on page 9 for rules concerning prefix and domain definitions, and more information on proxy server use.

8. Click Add to add entries to the list and OK to finish.

**Using a Proxy with GMA Secure Browser**

You can use an HTTP and/or HTTPS proxy with Secure Browser.
• HTTP proxy is used to connect to HTTP sites (non-SSL sites). The browser requests the page from the proxy by passing a full URL to it; the proxy checks the URL and fetches the page or sends it from its cache to the browser. The HTTP proxy will know the URL and content of pages flowing back and forth between browser and website.

• HTTPS proxy is used to connect to HTTPS sites (SSL sites), setting up end-to-end SSL connections. In this case, the browser will first set up an HTTP tunnel connection to the end website through the proxy server and then perform the SSL negotiation over the HTTP tunnel connection.

If an HTTP URL is entered, Secure Browser will use the HTTP proxy; if an HTTP proxy entry is not set, Secure Browser will try to connect without a proxy. If an HTTPS URL is entered, Secure Browser will use the proxy from the HTTPS proxy entry; if an HTTPS proxy entry is not set, Secure Browser will try to connect directly without using a proxy.

**Bypass Rules**

You can enter exceptions on the Settings > Secure Browser page for particular hosts of URLs.
URLs entered in the device’s secure browser for pages on these hosts cannot be reached via proxy. Enter the excepted hosts, separated by commas, using any of the following:

- Host names or fully qualified host names. Examples: kb, hub, hub.corp.acme.com. Note: Host name and fully qualified host name will not match with each other; enter both in the exceptions list if the user might enter either in Secure Browser.

- Domain names with wild card. Examples: good.com, *.good.com, .good.com. Formatting matches Firefox usage. The following formats are supported:

- IP addresses. Example: 192.168.1.2. If the secure-browser user enters a URL, Secure Browser will first try to resolve the IP address of the host using the Good Mobile Messaging Server and then match the IP address to the IP addresses in the exception list. If either Secure Browser is not able to resolve the IP or the IP does not match an IP in exception list, Secure Browser uses the proxy.

- IP address groups. Example: 192.168.0.0/16.

- allhostswithnodomain – If this keyword is included in the proxy bypass list, all URLs containing a non-fully qualified name (like https://testhost, https://hub, instead of https://testhost.good.com) will be excluded from proxy use.

If a host name is used instead of an IP address in the URL, Secure Browser matches the host to the list of host names in the allowed list of hosts sent from the Good Mobile Messaging Server. If the host is present in the list, Secure Browser will process it; otherwise, the user will be prompted to open the page in native browser. Note that the
host name in the exception list on the Settings page and the allowed list on the GMA policy page must match exactly.

If proxies are present, Secure Browser handles host names as follows:

- Matches the host name to the proxy exception list
- If the host name is matched with an entry in the proxy exception list, Secure Browser will try to connect without using the HTTP proxy.
- If the host name is not matched with an entry in the proxy exception list, but the exception list contains IP addresses, Secure Browser will first request the Good Mobile Messaging Server to resolve the IP address of the host name and then match it to the IP addresses in the exception list. If the IP address cannot be resolved or the received IP address does not match an entry in the exception list, Secure Browser will use the HTTP proxy server.

If an IP address is used in the URL, GMA decides whether to process it or launch Safari, using the following rules:

- If the IP address is a private IP, it is simply processed using Secure Browser
- If the IP address is public, it is matched to the allowed host list set in the Good Mobile Control Console (Plugin Policies > Good Mobile Access (Secure Browser)); if found, it is processed with Secure Browser; otherwise, native browser is launched. If the “Disable redirect to native browser” policy setting is enabled, GMA will inform the user.
- The IP address is matched with the proxy exception list. If the IP address is matched with an entry in the exception list, Secure Browser will connect without using HTTP proxy; otherwise, it will connect using the HTTP proxy.

Note: If a page host has more than one IP address, all such addresses should be entered in the proxy exception list. Secure Browser only matches the first IP address in a list of IPs sent from a host server to the proxy exception list; entering all the host addresses assures that the exception will be recognized.

Authentication types supported for proxies
Secure Browser supports the following HTTP/HTTPS proxy authentications:

- Basic
- Digest
- NTLMv2
- Kerberos

Good recommends using NTLM, as Basic authentication involves sending plain passwords to the proxy server. Anyone sniffing data between Good Mobile Messaging Server and the HTTP proxy server can discover such a password.

The authentication will be cached in the program memory of the application and will not prompt the user for subsequent access until the application is restarted. Every time the application is restarted (after being killed manually or by OS) the user will be prompted for credentials when accessing the proxy.
Usability

Users may ask why they have to enter their domain credentials so often to access intranet sites.

• Good does not cache authentication credentials.
• If a Good Client session has expired or terminated, the user will need to authenticate the session again.

Your remote application/server may also have a timeout value. Note also that if a user requires a client certificate when using GMA Secure Browser, they can visit the Good Mobile Control Self Service page and download an identity certificate to their device.

Android

ROM 2.3:

Mozilla/5.0(Linux; U; Android 2.3.5;en-us;ME860 Build/4.5.3-118_OLY_14) AppleWebKit/533.1 (KHTML, Like Gecko) Version/4.0 Mobile Safari/533.1

ROM 4.0/4.1/4.2/4.3

Mozilla/5.0(Linux; U; Android 4.2;en-us;Galaxy Nexus Build/JDQ39) AppleWebKit/534.30 (KHTML, Like Gecko) Version/4.0 Mobile Safari/534.30

iOS

Iphone 4 (6.1.3)

Mozilla/5.0(iPhone; CPU iPhone OS 6_1_3 like Mac OS X); AppleWebKit/536.26 (KHTML, Like Gecko) Mobile/10B329 Safari Version/6.0; Your IP Address: 206.124.127.15

Iphone 5s (7.0.4)

Mozilla/5.0(iPad; CPU iPhone OS 7_0_4 like Mac OS X); AppleWebKit/537.51.1 (KHTML, Like Gecko) Mobile/11B554a Safari Version/6.0; Your IP Address: 206.124.127.15
Ipad4 (7.0.6)
Mozilla/5.0(iPad; CPU iPhone OS 7_0_6 like Mac OS X); AppleWekbit/537.51.1 (KHTML, Like Gecko) Mobile/11B651 Safari Version/6.0; Your IP Address: 206.124.127.15

Good Mobile Access within Good For Enterprise version 2.1
iOS/Android Secure Browser Feature Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>iOS</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported OS versions</td>
<td>iOS 5.0+</td>
<td>Android OS 2.3+</td>
</tr>
<tr>
<td></td>
<td>GMA 2.1 does not support iOS 4.0.</td>
<td>GMA 2.1 does not support Android 2.2.</td>
</tr>
<tr>
<td>Mail server support</td>
<td>Exchange and Domino</td>
<td>Exchange and Domino</td>
</tr>
<tr>
<td>HTTP basic authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTP digest authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NTLMv2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NTLMv2 session</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTP 1.1 protocol</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS and SSL</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Encryption of cache, bookmarks, history, and downloaded files</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>End to end encryption of data using AES 192 bit encryption</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bookmarks</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Homepage</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>History</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Full screen mode</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>iOS</td>
<td>Android</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>HTML5 support</td>
<td>Most of the HTML5 elements and javascript are supported, except for embedded video and storage APIs</td>
<td></td>
</tr>
<tr>
<td>AJAX support</td>
<td>Yes, however synchronous AJAX requires using iOS 5</td>
<td>Yes</td>
</tr>
<tr>
<td>Multiple windows support</td>
<td>Yes (in Prevue 2.2 only)</td>
<td>No</td>
</tr>
<tr>
<td>Pop-up window support</td>
<td>Yes. However, pop-up window (self or new) replaces current window. JavaScript logic testing for the pop-up will not work. There is no setting to block pop-ups. “Back” returns to parent page.</td>
<td>No</td>
</tr>
<tr>
<td>Proxy support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Client certificate support using SSL mutual authentication</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Flash support</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Allow/Block NFQD access policy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support disabling of directing user to Native Browser</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSL Server Certificate Validation</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Save website documents into GFE Docs Repository</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Open website documents in other applications</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Tabbed browsing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
SSL Server Certificate Validation
GMA iOS only, using GFE iOS Client 2.1.

For security purposes, GMA iOS performs validation on the SSL Server certificate.

This feature requires the root certificate to be available on the device’s key store. For GMA to consider the certificate as valid:

- Or the root certificate is put into the device keystore via a solution such as Good Management Control’s Mobile Device Management feature. Deploy the root certificate to the device keystore by creating a WIFI (Enterprise) profile.

To turn this security feature off, add the keyword, "disablecertwarning.gmm.good" (without quotes) to the list of allowed domains via the "Allow access to the following Intranet domains” option within the Good Management Console.

If the SSL server certificate is considered not valid by GMA or has expired, users can choose whether or not to continue to access the website. If a user elects to "Continue" onto a website after the warning, that user’s preference persists after the Good For Enterprise client restarts or is upgraded. If the user selects "Cancel" after being prompted, Secure Browser will prompt the user when the user goes back to the website again. The user is also able to see the details of the certificate when prompted.

If the user selects "Cancel" when notified that the SSL server certificate for that web server is not validated, and returns to the website again, GMA will prompt the user again to see if the user wants to continue to access the website.
Client Certificate-based Authentication Support

This feature is for customers wanting to use soft token-based mutual authentication by using identity certificates.

**Note:** iOS only, using GFE iOS Client 2.1.

- Only one identity certificate supported per user/device. One certificate can be used across all websites requiring soft-token mutual authentication.)
- GMA will alert the user if the certificate has expired or has been revoked based on information from the authentication server or web server.
- GMA is able to use this certificate only for SSL mutual-based authentication, not for Kerberos client certificate-based authentication. However, a Kerberos identity certificate can be used.
- The identity certificate, including the private key, is stored in the Good For Enterprise app’s secure container.
- The Self Service Portal enables users to upload identity certificates. The Self Service Portal is also required for users to use the “Upload identity certificate” features.

**Identity Certificate Deployment Flow Using the GMC Self Service Portal:**

**Outside of Good**

- The user obtains an identity certificate, exported from a desktop app such as Internet Explorer (Internet Explorer -> Internet Options -> Certificate). The user must export the private key as well. The exported file is a PKCS#12 certificate (.p12 or .pks file). The user encrypts this PKCS#12 certificate using a password/PIN. This is the password/PIN that GMA will use to install the certificate for use by GMA.

**On Good Management Console (GMC)**

- The IT admin sets a role allowing the user to enable “Upload identity certificate.”
On GMC Self Service Portal
• The user uploads the identity certificate.

In the Good For Enterprise app
• Secure Browser in the GFE app receives the identity certificate after the user has uploaded it via the Self Service Portal. Secure Browser prompts the user to install the identity certificate with their certificate encryption password/PIN. The user can choose to install the identity certificate later, at a time when a website requests an identity certificate.

How Secure Browser Uses the Identity Certificate

In the Good For Enterprise app, when Secure Browser gets a request from a website for a client certificate for mutual authentication, Secure Browser will:

• Look for an installed certificate for the user in the secure container.
• If there is no valid secure certificate installed, the Secure Browser looks for an identity certificate yet to be installed in the secure container. It will prompt the user to install the certificate.
• Once an identity certificate is found, the Secure Browser prompts the user for “Always trust” if they want to use that identity certificate every time they try to access that website. Good app’s Secure Browser will not ask the user to use the identity certificate for that website again even after the Good app restarts, until the identity certificate expires or is revoked.

If the identity certificate has expired or been revoked, the user can upload another identity certificate via GMC’s Self Service Portal.

Disabling Redirection To Native Browser

The IT admin can block users from being passed to the native browser (Safari on iOS) by enabling the option “Redirect domains not listed above to native browser” in the policy section of the Good
Mobile Control Console. With this policy setting, users will no longer see the “Open In Native Browser” option when the website is not on the allowed domain list in the policy. A standard message saying “The website you are trying to reach is blocked due to IT Security policy” will be displayed. Enabling this policy does not mean that the web traffic will go through GMA if the web server is on a domain not on the GMA allowed domain list. Instead, the user will receive a message that the website is blocked due to IT Security Policy.

**Saving a Document to the Repository and Opening the Document in Another Application**

In Secure Browser, the user can:

- Save files on websites to the Good For Enterprise document repository on the device.
- Open files on websites using IT policy-compliant native and Good Dynamics applications.

Documents not supported:

- HTML/HTM files
- Image files not reachable at the top-level URL (for previewing)
- Files not accessible via the top level URL. Example: Word Document and Powerpoint files on Sharepoint 2003 and 2010 with Office Web Apps enabled.

Files are previewed in Secure Browser before the user is able to click on an Action icon at the top right of the screen, to bring up the menu items “Save As” or “Open In.” Excepted are audio/video files where users will not be able to preview the file via GMA first but are asked if they want to download it into Docs Repository for listening/viewing).

**Troubleshooting**

Q: Are there any debugging commands for GMA Secure Browser?

A: The following commands can be entered in the GMA secure browser to help troubleshooting issues.
However, note that the Secure Browser debug commands (for example, debug://policyprint for iOS and sbdebug://policyprint for Android) will not function by default.

To enable the debug commands, a new GMC setting is required. Under a device’s Good For Enterprise policy set, on the Good Mobile Access (Secure Browser) page, a new string must be added to the “Allow access to the following Intranet domains” list:

`enableddebugcommands.gmm.good`

Once this updated policy syncs to the client, the debug commands on GMA will function as desired.

**iOS**

debug://policyprint displays policy set in a server, this is helpful in determining access rights and domains that are allowed.

default://listfailedhosts display list of domain names that are causing problem for GMA to load.

default://loglevel:65355 sets higher level of logging. Logs can be sent to Good by going to Preferences/About

default://cachecleanup cleans up the stored browser cache so GMA can download the latest webpages from the web server

**Android**
sbdebug://policyprint displays policy set in a server, this is helpful in determining access rights and domains that are allowed.

sbdebug://listfailedhosts display list of domain names that are causing problem for GMA to load.

sbdebug://loglevel:t:4064 sets higher level of logging. Logs can be sent to Good by going to Preferences/About

sbdebug://clcache cleans up the stored browser cache so GMA can download the latest webpages from the web server

Q: Why am I getting an error message in GMA Secure Browser but not in Safari when I access a website?

A: It could be an issue with AJAX based requests. Follow the steps below to report issues to Good,

1. Go to GMA Secure Browser
2. Enter debug://loglevel:65355 (for iOS) or sbdebug://loglevel:t:4064 (for Android) in the address bar, then press Return.
3. After that clear the address bar and access the site.
4. Continue testing.
5. Once testing is done, go to Preferences/About and upload logs.

Q: Why is the secure-browser icon not displayed on the user’s device?

A: Check the following:

- For Android devices, is the required 2.2, 2.3, 4.0, 4.1, or 4.2 OS present?
- Is GMA enabled on the Settings page in Good Mobile Control? (GMC 2.2 or earlier. GMC 2.3 removes this setting.)
- Is GMA Policy Enabled and added to this handheld?
- Have you waited for the Policy Update Delay to expire?
- Try completely exiting Good Client (kill the background task) and launching again.
• Restart Good Mobile Messaging and Good Mobile Control Services.

Q: When a user attempts to navigate to a domain that I have allowed, he/she receives a “Failed hosts identification” message. Why?

A: Use the browser to navigate to

iOS
debug://listfailedhosts

Android
sbdebug://listfailedhosts

Check the domain names that are causing the problem. Confirm that you have allowed them in the policy. These may include, for example, embedded internet sites that are referenced on your intranet pages.

If a domain is properly listed in the policy but is causing access problems, confirm the following:

• Can Good Messaging Server connect to the requested host.
• Can Good Messaging Server resolve the host name to an IP address through DNS lookup?
• Can Good Messaging Server connect to the resolved IP address and requested port number?

The device screen should be kept on during secure browsing. The user may encounter an error if the device goes to sleep during browsing.

Q: Why am I encountering Kerberos error code = -1765328230?
A: In general, this error occurs if you entered the incorrect realm. When entering credentials for Kerberos authentication, ensure that the domain field contains the full realm name.

Q: I’ve applied a Kerberos configuration file to the Good policy, but I’m still getting NTLM authentication requests. How I can troubleshoot the issue and see the logs where the failure occurred?

A: Try the following:

1. Remove dns_lookup_kdc and dns_lookup_realm from the configuration file.

2. Add the hosts found in the Kerberos configuration file under KDC to the allowed domain list in GMC under the GMA Secure Browser policy. For example, for krb5.conf:

   ```
   [libdefaults]
   default_realm = GMMEXCH.QAGOOD.COM
   [capaths]
   GMA.QAGOOD.COM = {
   GMMEXCH.QAGOOD.COM=.
   }
   GMMEXCH.QAGOOD.COM= {
   GMA.QAGOOD.COM=.
   }
   ```

   Add GMMEXCH.QAGOOD.COM and GMA.QAGOOD.COM to allowed domain list in GMC.

3. Ensure that Kerberos is enabled in GMC.

4. In the client Secure Browser, type debug://ktools. A console is displayed. In the console, do the following:

   a. Type config to check that the correct config file is present on the device. Convert all domains to caps.

   b. Try fetching TGT tickets using the kinit command line. Use caps for all domains.

   c. Try fetching service tickets using the kvno command line.

   Note that for Kerberos to be used for any site, the client needs to know the realm for the site that the client is trying to authenticate. For example, for "test.domain.good.com."
Use the configuration file to provide this information. You can update the section domain_realm with

```
domain.good.com = GMA.QAGOOD.COM
domain.good.com = GMA.QAGOOD.COM
```

This assumes the GMA.QAGOOD.COM KDC server does the authentication for test.domain.good.com. Once you make the change, you can confirm with a "config" command and then try:

```
kvno HTTP/TEST.DOMAIN.GOOD.COM
Clear tickets using kdestroy.
```

**Frequently Asked Questions**

**General**

Q: What is Good Mobile Access (GMA) Secure Browser?

A: GMA secure browser allows mobile access to enterprise web applications without the need of VPN.

Q: What is the benefit of GMA Secure Browser over native browser via VPN?

A: GMA Secure Browser provides secure storage and encryption while native browsers do not. Also, using native browsers via VPN allows any third party applications on the device to access the intranet, whereas GMA Secure Browser would restrict access to only the GMA client.

Q: What platforms does GMA Secure Browser support?

A: GMA Secure Browser is available on: iPhone, iPod Touch and iPad using Good iOS client 1.8.3 with iOS 4.0 and above; Android devices using the 2.2, 2.3, 4.0, 4.1, and 4.2 OS.
Q: What do I need to deploy GMA Secure Browser?
A: Good Mobile Messaging server 6.3.1 or higher (Exchange) and Good Mobile Control server 1.3.1 or higher; or Good Mobile Messaging server 6.3.1.74 or higher (Domino) and Good Mobile Control server 1.3.1.122 or higher. To enable GMA Secure Browser, go to GMC Settings tab and click on the "Good Mobile Access (Secure Browser)" setting, then select the checkbox to Allow Intranet Access from the server. You'll also need to configure domain list through policy, see Administrator's Guide for more details.

Supported Technologies

Q: Which web servers does GMA Secure Browser support?
A: We have tested with IIS 6.x and 7.x and the latest version of apache. As long as web servers support HTTP 1.1 spec, they should be compatible with GMA Secure Browser.

Q: Is GMA Secure Browser built on WebKit?
A: Yes, GMA Secure Browser uses the same WebKit as used by Safari and Android native browsers, therefore rendering HTML pages should be identical. However, there are some differences between GMA Secure Browser and Safari and Android native browsers because the communication between client and Good's NOC and how AJAX requests are being handled.

Q: Does GMA Secure Browser support HTTPS and SSL?
A: Yes, they are supported by GMA Secure Browser. However, GMA Secure Browser would not display warnings if SSL certificate is invalid. Note that GMA does not support SSL 3.0 by default. For 3.0, add "ssl30only.gmm.good" to the list of allowed domains via the "Allow access to the following Intranet domains" option within the Good Management Console.

Q: Does GMA Secure Browser support HTTP 1.1 protocol?
A: Yes, GMA Secure Browser supports HTTP 1.1 protocol as per the RFC spec. This includes GET/POST, redirection, cache directives, transfer-encoding, authentication status, and gzip support. Advanced HTTP protocols like web sockets and HTTP pipelining are not supported.

Q: Does GMA Secure Browser support HTML5?
A: GMA currently supports HTML4 and the HTML5 features indicated in the separate document “Support for HTML5 and CSS3.”

Q: What are some of the best practices for developing websites for GMA Secure Browser?
A: Avoid embedding HTML pages inside <object> tags and don’t rely on having a website and a pop-up window open at the same time. Websites should also detect and optimize the content layout if they are accessed from an iPhone.

Q: Does GMA Secure Browser support NTLM v1 & v2 authentication?
A: The latest version of Good iOS client only supports NTLM v2 authentication.

Q: Does GMA Secure Browser support HTTP basic and digest authentication?
A: HTTP basic and digest authentication are supported in the latest version of Good iOS and Android Clients.

Q: Does GMA Secure Browser support web cookies?
A: GMA Secure Browser supports web cookies. Depending on cookie type (memory or persistent), the cookie could be erased when user exits Good client.
Q: Does GMA Secure Browser support Single Sign-On?
A: GMA supports cookie- and Kerberos-based single-sign-on. GMA iOS supports certificate-based authentication via SSL.

Q: Does GMA Secure Browser support caching of login session?
A: Yes, GMA Secure Browser caches login session for NTLM v2, HTTP basic and digest authentications. The cache is cleared when user exits Good client.

Q: How long would GMA Secure Browser cache the login credentials? Is there a way to specify how long it can be cached?
A: GMA caches the login credentials only for the application session, they are cleared when user exits Good client.

Q: How does GMA Secure Browser work with intranet websites that require user login? Does user need to enter user name and password every time?
A: When user visits a website that requires user login for the first time, GMA will prompt user for the login credential. Subsequent visits to that website will not require user to re-login until user exits Good client, at which point the cache is cleared. Login credentials are unique to each website; they are not shared across multiple websites.

Q: Does GMA Secure Browser support ITPC protocol for loading iTunes podcasts?
A: No, GMA Secure Browser only supports HTTP and HTTPS protocols.

Q: Does GMA Secure Browser support using proxy server or Auto Proxy?
A: GMA Secure Browser on iOS supports proxy server but not PAC file. GMA Secure Browser on Android also supports proxy server but not PAC file.
Q: Does GMA Secure Browser support Apple Specific Meta Tags?
A: No, GMA Secure Browser does not support using any Apple Specific Meta Tags.

Best Practices

Q: How many GMA Secure Browser users can be supported on a GMM server?
A: GMM server can support up to 1,050 GMA Secure Browser users concurrently (assumes 20% are using GMA simultaneously). GMM server is a 32-bit application which has a 2GB Virtual Memory limit, and in an ideal situation, the memory usage should be around 1.5GB. Limiting usage to 1,050 GMA Secure Browser users on a GMM server ensures that memory usage will not exceed 1.5GB during normal load conditions, with sufficient memory to handle high load conditions.

Q: Can GMA Secure Browser access intranet websites that has references to external URLs?
A: External URL domains can be added to the list of allowed domains through GMC’s policy, so content hosted on external website can be displayed through GMA Secure Browser.

Q: What can I do to ensure that my intranet websites are built to support GMA Secure Browser?
A: Your intranet websites should not use the features that are not supported in GMA Secure Browser, such as embedded HTML pages. See the Supported Technologies section for a list of supported and unsupported features.

Usage Scenarios

Q: Can GMA Secure Browser access external internet websites?
A: If an external website is listed as one of the allowed domains in the policy, then it can be accessed through GMA Secure Browser. If it is not listed as one of the allowed domains, users will be prompted to open the website with the native browser. Web pages accessed outside GMA Secure Browser will not be stored in the secure container.

Q: Can GMA Secure Browser access Sharepoint?
A: Yes, Sharepoint can be accessed via GMA Secure Browser, as long as it is listed as one of the allowed domains in the policy.

Q: When I access a file on Sharepoint using GMA Secure Browser, is the content stored securely?
A: Yes, everything downloaded through GMA Secure Browser is stored in a secure container, including any files, images downloaded through Sharepoint or any other intranet websites.

Q: What information is encrypted through GMA Secure Browser?
A: GMA Secure Browser encrypts webpages, bookmarks, browser history, cookies, and cache.
Document Revision List

09/06/12

Added pop-up window support.

Added to Troubleshooting section of FAQ a Kerberos Q&A regarding Kerberos configuration file and continued NTLM requests.

11/05/12

Typos corrected.

02/05/13

New in GMA with GMC 2.3.0

- **Compliance with “Disable Redirect to Native Browser” policy** – IT admin may set a policy to not allow redirecting the user to Safari. If the website is not part of the allowed list, then the end user will see the prompt “The website you are trying to access is blocked by IT security policy.” (Requires GMC 2.3.0) (“Enabling Secure Browser” on page 7)

- **Compliance with blocking of Non-fully qualified domain (NFQD) policy** - IT Admin may set a policy to not allow users to get to non-fully qualified domains. (Requires GMC 2.3.0) (“Enabling Secure Browser” on page 7)

- **SSL Server Certificate Validation** – For added security, GMA will alert the user if the SSL server certificate on the server is not valid (i.e. expired). GMA will allow a user to decide to continue with accessing the website.

- **Compliance with policy to disallow access to websites with non-valid server SSL certificates** - GMA will comply with the new GMC flag which could block accessing websites with invalid SSL server certificates. (Requires GMC 2.3.0 server) (“Enabling Secure Browser” on page 7)
• **Save Files From Websites to Docs Repository** – Download files (office documents, pdfs, and media files) to the Docs repository of Good For Enterprise app. This requires GMC File Repository policy to be Enabled.

• **Open Files From Websites via 3rd Party Apps (Good Dynamics applications)** – Be able to open files (office documents, pdfs, and media files) using Good Dynamics and other third party applications based on IT policies. This feature depends on policies on GMC.

• **SSL client certification authentication** – Support mutual authentication using SSL client certificates (soft token). (Requires GMC 2.3 and Self Service Portal)

• **Support for Phone Number Dialing and Email Compose from websites** - Phone numbers and email addresses on websites are now highlighted and actionable (for making phone calls and email compose via Good For Enterprise)

• **Better URL/progress bar user experience** - GMA will display the url progress bar when user clicks on a url on a page.

• **Additional Kerberos Configuration Support** - Support for additional Kerberos configurations. (“Using Kerberos Authentication” on page 4)

03/08/13

Enhancing the explanatory material for the new 2.3.0 features listed above.

05/22/13

Updated HTML5 support matrix and moved it to a separate document.

08/21/13

Added additional technical information throughout the guide.