

Good™ Mobile Messaging Good™ Mobile Control

Wireless Enterprise Messaging and Data Access System

Secure Browser Guide

Good for Enterprise

Legal Notice

This document, as well as all accompanying documents for this product, is published by Visto Corporation dba 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 2011. 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.
101 Redwood Shores Parkway, Suite 400
Redwood City, CA 94065

<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
Enabling Secure Browser	5
<i>Usability</i>	7
Frequently Asked Questions	8
<i>General</i>	8
<i>Supported Technologies</i>	8
<i>Best Practices</i>	12
<i>Usage Scenarios</i>	12
<i>Troubleshooting</i>	13

Secure Browser (Good Mobile Access)

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.

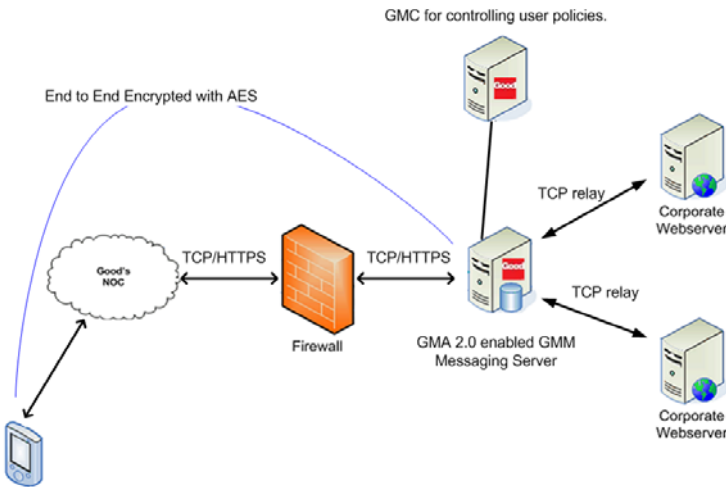
The secure browser provides a browser history, which can be cleared. Naming and editing bookmarks is supported. The browser supports pinch and zoom, and landscape mode. No special training is required.

Secure Browser supports HTML 4.

Overview

Secure browser provides browsing-only functionality for iOS 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
- Remote wipe of cache, bookmarks, history, downloaded files, etc.
- 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 does HTTP transaction (POST/GET). Good Messaging server will simply pass the data to and fro 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
- Good Messaging Server does not support connection to hosts through proxy servers

In addition:

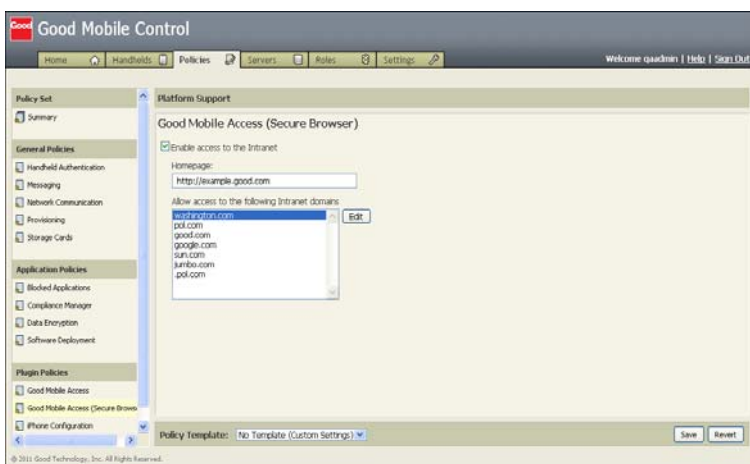
- Secure browser requires the Good iOS Client 1.8.2. No other iPhone or iPad preparation is required.
- NTLM v2, and HTTP basic and digest authentication are supported.
- If all users are using secure browser, a Messaging Server can handle up to 600 users.

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.

Enabling Secure Browser

To enable Secure Browser for users via a policy:

1. First go to the Good Mobile Console Settings tab and click on the Good Mobile Access link in the left panel. On the Good Mobile Access page that is displayed, click the Enable checkbox.
2. To set policies for intranet browser use, 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.



(If using Secure VPN with Windows Mobile devices, the screen will be slightly different.)

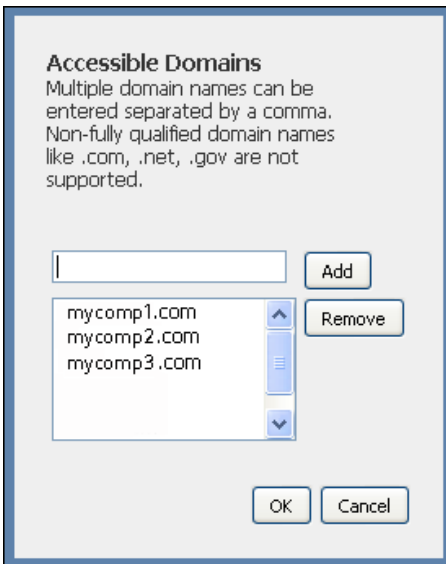
3. Click the “Enable access to the intranet” checkbox to turn on the browser feature for supported handhelds using this policy (and to display the full screen above).

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

4. 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.
5. 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 are supported by default, with the exception of names such as .com, .net, .gov, and .edu.

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.”

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

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.

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 Safari via VPN?

A: GMA Secure Browser provides secure storage and encryption while Safari does not. Also, using Safari 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.

Q: What do I need to do to deploy GMA Secure Browser?

A: Good Mobile Messaging server 6.3.1 and Good Mobile Control server 1.3.1 for Microsoft Exchange are needed to deploy GMA Secure Browser. 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, therefore rendering HTML pages should be identical. However, there are some differences between GMA Secure Browser and Safari because the communication between client and Good's NOC and how AJAX requests are being handled. See "What differences are there between GMA Secure Browser and Safari?" for a list of differences.

Q: What differences are there between GMA Secure Browser and Safari?

A: Here are some of the different behaviors between GMA Secure Browser and Safari

- Embedded HTML pages placed in <object> tags may not render properly, due to a bug with Apple's WebKit.
- Safari displays warning to user for invalid SSL certificates, but GMA does not display warning.
- GMA Secure Browser can only have one website open at a time, so any pop-up window would close the website behind it. Websites running JavaScript to detect open pop-up would fail.
- Good Secure Browser uses custom protocol to communicate with Good's NOC, this causes issues handling synchronous AJAX based requests. Only asynchronous AJAX calls are supported. See troubleshooting section on how to log and report issues with AJAX websites.

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.

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 only supports HTML 4.

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 client.

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 based single-sign-on, but certificate and Kerberos based single-sign-on are not supported.

Q: Does GMA Secure Browser support caching of login credentials?

A: Yes, GMA Secure Browser caches login credentials 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: No, GMA Secure Browser does not support using proxy server.

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 600 GMA Secure Browser users concurrently. 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 600 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 and pop-up windows. 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 Safari. 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, and browser history.

Troubleshooting

Q: Why is GMA Secure Browser not able to handle NTLM authentication? It is caught in a loop prompting my login credential over and over.

A: There could be two possible issues with NTLM authentication:

- If web server sends challenge with some content, it would cause an issue with older clients of Good. This issue has been fixed in the latest version of Good client 1.8.3.
- If web server's registry setting "HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA\MSV1_0\NtlmMinServerSec" has flag "0x00080000-NTLM 2 session security" set then client will not be able to authenticate. It needs to be changed so that "0x00080000-NTLM 2 session security" is not present. For example, if your current NtlmMinServerSec is set to "0x20080030" then change it to "0x20000030". To enhance security even without this flag, the flag "HKEY_LOCAL_MACHINE\System\CurrentControlSet\con

trol\LSA\LMCompatibility" can be set to accept NTLMv2 connections only.

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

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

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

debug://loglevel:65535 sets higher level of logging. Logs can be sent to Good by going to Preferences/About

debug://cachecleanup 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:65535 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:

- Is GMA enabled on the Settings page in Good Mobile Control?
- 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

```
debug://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?
- Is the connection to the host accomplished through a proxy server? This is not supported.

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

