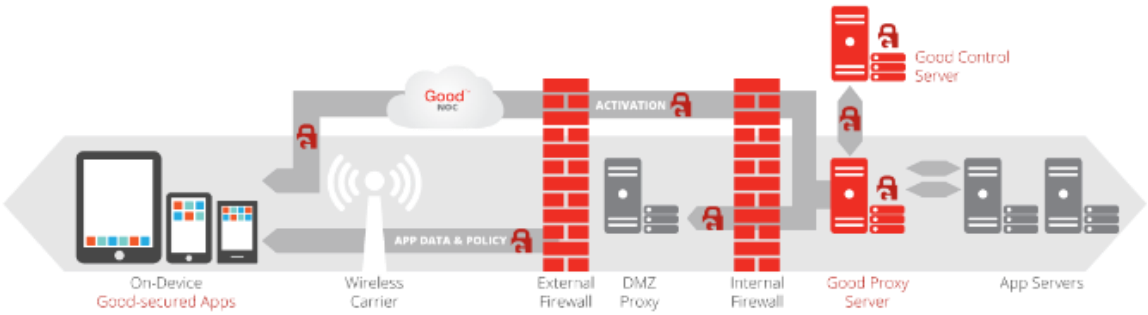
QlikView for Good

Good Technology

Good Technology provides infrastructure that enables Mobile device users to securely access confidential content within their Intranet. There are several components to the Good Dynamics solution:

- Good Control
- Good NOC
- Good Proxy
- Good clients
- Good Community

If the QlikView AccessPoint Portal is hosted in a DMZ, then it is possible to connect to it using the native browser or the **QlikView for iOS** client. When firewalls prevent direct connectivity to QlikView AccessPoint then it is necessary to interact with it using the **Good Access** browser or the **QlikView for Good** client.



Good Control (GC)

The **Good Control** component provides the administrative interface for configuring the entire Good environment. Within **Good Control** you identify Users, their devices, Policies affecting those Users, which Applications are recognized for use by those Users [regardless of device being used], configuration properties of the applications, and which internal servers are whitelisted for access via the **Good Proxy**. If a device is lost or the user should no longer have access to a particular application then **Good Control** is used to revoke that access.
Changes are propagated out to the **Good NOC** as a First Point of Contact for the mobile devices.

Good Network Operations Center (NOC)

The **Good NOC** is what Good client applications first connect to when activated. Though the user has identified themselves to their device using a PIN or perhaps a fingerprint, Good client applications must authenticate themselves to the NOC, from which they then determine the address of the **Good Proxy** through which they will connect for access to particular content. If use of an application has been revoked, then the device determines this from the NOC and will erase all local content.

Good Proxy (GP)

This component is the bridge between external devices and internal services.
Though the name suggests an intermediary that accepts incoming connections then performs an onward connection to the requested content, the **Good Proxy** actually operates as a *Gateway* for connections that are tunneled over HTTPS from applications on the mobile device to servers within the customer's network. The **Good Proxy** is NOT a generic VPN tool that enables *any* traffic from the device into the corporate network, however Good does provide the ability to manage those settings on the mobile device.

The **Good Proxy** can also insert a Kerberos token into the tunneled traffic, to provide seamless authentication from the mobile application to the target service.
Connectivity from mobile devices to the GP is performed on 17533/tcp or via NOC on 443/tcp.

Good clients

Good client applications are built upon the Good Dynamics Secure Mobility Platform APIs which provide features such as authentication, secure data transfer, secure storage, remote wipe, and more.

- **Good Access** – secure browser
  https://www1.good.com/applications/collaboration-suite/good-access/
- **Good Work** – email, contacts, calendar and meeting client
  https://www1.good.com/applications/good-work/
- **Good Share** – search/sync content from Microsoft SharePoint
  https://www1.good.com/applications/collaboration-suite/good-share/
- **Good Connect** – manage contacts, determine availability and chat with them
  https://www1.good.com/applications/collaboration-suite/good-connect/

These and other applications can be downloaded from an AppStore or from a private Enterprise AppStore.

- iOS https://itunes.apple.com/us/app/good-for-enterprise/id333202351
- Android https://play.google.com/store/apps/developer?id=Good+Technology
- Windows http://apps.microsoft.com/windows/en-gb/app/d75afd5a-09ac-4338-9157-1063b776a2df

Though a user may download an application to their mobile device, the device must be enrolled with the enterprise, the application must be recognized on **Good Control** and associated with the user. When successfully enrolled, the device will have a Certificate pushed to it which is used for authentication to the NOC. The NOC will deliver configuration profile and settings such as VPN and WiFi configuration. After enrolment, the address of the **Good Proxy** and other application-specific properties are delivered when the client application is started.

- Good Device and Application Management
  https://community.good.com/docs/DOC-3868

A user's access to an application can be changed at any time [via GC] and is enforced next time the application is started.

Good Community

The Good Community https://community.good.com/ contains documentation, and forums for discussion Good-related issues. It is also where you will register for access to applications.

- Good Marketplace
  https://community.good.com/marketplace.jspa
- Good Dynamics Platform Overview for Administrators and Developers
  https://community.good.com/docs/DOC-1061
  - pp10: A new employee requires an enterprise application
  - pp10: An employee loses a device
- Good Dynamics Server Installation
  https://community.good.com/docs/DOC-1043
- Good Dynamics Kerberos Constrained Delegation (KCD)
  https://community.good.com/docs/DOC-2716

Upon initiating a Trial of **QlikView for Good** via Marketplace, a registration is submitted to Qlik, and must be activated via https://community.good.com/groups/qlik by a member of Qlik staff.

QlikView

QlikView is a Business Intelligence tool in the Data Visualization niche. It provides a "Managed Analysis" capability allowing the user to navigate and filter freely on any of the objects in a rich multi-sheet dashboard. All visible objects are recalculated after a user performs selections (green) causing ***associated*** (white) data to be clearly distinguishable from non-associated (grey) data.

There are several components to a QlikView implementation:

- QlikView Management Service (QMS)
- QlikView WebServer (QvWS) or Microsoft Internet Information Server (IIS)
- QlikView Directory Service Connector (DSC)
- QlikView Server (QvS)
- QlikView Distribution Service (QDS) "Publisher"
- QlikView Desktop
- Browser clients
- Qlik Community

Typically, the only component that the Good Dynamics infrastructure needs to provide connectivity to is the WebServer, however in some environments it may be appropriate to provide the QlikView Management Console also.

QlikView Management Service (QMS)

The QlikView Management Service provides an HTML interface for the configuration and administration of the entire QlikView environment. Only one QMS should be active per environment.

- Authentication is supported using NTLM and HTTP Basic mechanisms.
  Only members of the Windows-local group "QlikView Administrators" are permitted access to the QlikView Management Console (QMC)
- Traffic to the QMC is HTTP on 4780/tcp, though API clients may connect on 4799/tcp.

Typical URL:

- QlikView Management Console (QMC) http://publisherHost:4780/QMC

The QMC is used to administer the accessibility (ACL) of QlikView documents on the QlikView Server, when those documents are refreshed with new data, and control which QlikView documents may have content cached to a mobile device for offline access.

QlikView WebServer (QvWS)

QlikView includes a WebServer for delivery of the QlikView "AccessPoint" portal and AJAX interface to the QlikView Dashboards. Microsoft IIS may be used in place of the embedded QvWS.

- Authentication is typically performed by Web Infrastructure between the Browser client and the website using Windows Integrated Authentication (Kerberos/NTLM), using trusted HTTP Headers inserted by Proxy infrastructure, or integration with a Forms Authentication tool. More sophisticated authentication is possible using Session Tokens requested by other infrastructure such as an alternate Portal.
  - QvWS is capable of NTLM, HTTP Basic and Header Authentication
  - IIS is required for Kerberos or Client Certificate Authentication or when using CA SiteMinder for Header Authentication. Care should be taken to adjust the scope of Authentication and select appropriate Authentication Methods. The *Negotiate* provider for *Windows Authentication* should be disabled.
- Traffic to the AccessPoint is typically HTTP on 80/tcp from a Javascript and HTML5 enabled Browser, or the **QlikView for iOS** client, or the **QlikView for Good** client. It is viable to use HTTPS 443/tcp but then generally IIS will be used because it includes tools for managing Certificates.
- Traffic to the AccessPoint website may be Load Balanced, but "Sticky Session" should be configured to ensure session contiguity to the same webserver where identity tokens are held.
- An additional 64bit component **QlikView Offline Service** must be installed on the WebServer if the Offline capability is required. This is not necessary for access using **Good Access** or simple non-offline content delivery using **QlikView for Good**

Typical URL:

- QlikView AccessPoint Portal http://webserverHost/qlikview/
- URL configured on **QlikView for Good** http://webserverHost

QlikView Directory Service Connector (DSC)

The DSC provides an interface to the User Repository – typically Active Directory but other LDAP types and Databases are also supported. This component is typically installed on the WebServer host, and listens on 4730/tcp for connections from the WebServer, QMS, and Publisher.

Multiple instances of the DSC may be implemented to support Failover.

QlikView Server (QvS)

The QlikView Server is the engine for delivery of the data underlying the Visualization, and is typically a large machine [or cluster] with sufficient RAM to hold the required data in memory for the visualizations that are in use, and many CPU cores for a large concurrent User community interacting

with those visualizations. Scale up with growing Data Volumes; scale out over multiple 2-4 socket hosts for a growing User Community.

Several QlikView Servers may be clustered at application-level (no 3rd party clustering software required), and load distribution is performed by the WebServers. A Windows FileServer is required for hosting content shared amongst the cluster nodes.

User interaction with the QlikView Servers is only via the WebServers (4747/tcp, 4774/tcp); Administrative traffic occurs from the QlikView Management Service, and possibly upload of Reloaded Documents from the QlikView Distribution Service(s).

QlikView Distribution Service (QDS)

The QlikView Distribution Service is also known as the “Publisher” or “Reload Engine”. This component performs the periodic reloading of QlikView documents with new data [from related databases, flatfiles or webservices] as a mechanism for staging the data into RAM on the QlikView Servers.

These may also be clustered if many QlikView documents need to be refreshed concurrently, or to achieve High Availability. There is no User Interaction with the QDS – merely administration via QMS.

QlikView Desktop

The QlikView Desktop is a Windows thick-client application used to create the QlikView documents which will be refreshed with data by the QDS, and deployed to the QvS for on-demand delivery of content to browser users.

Browser clients

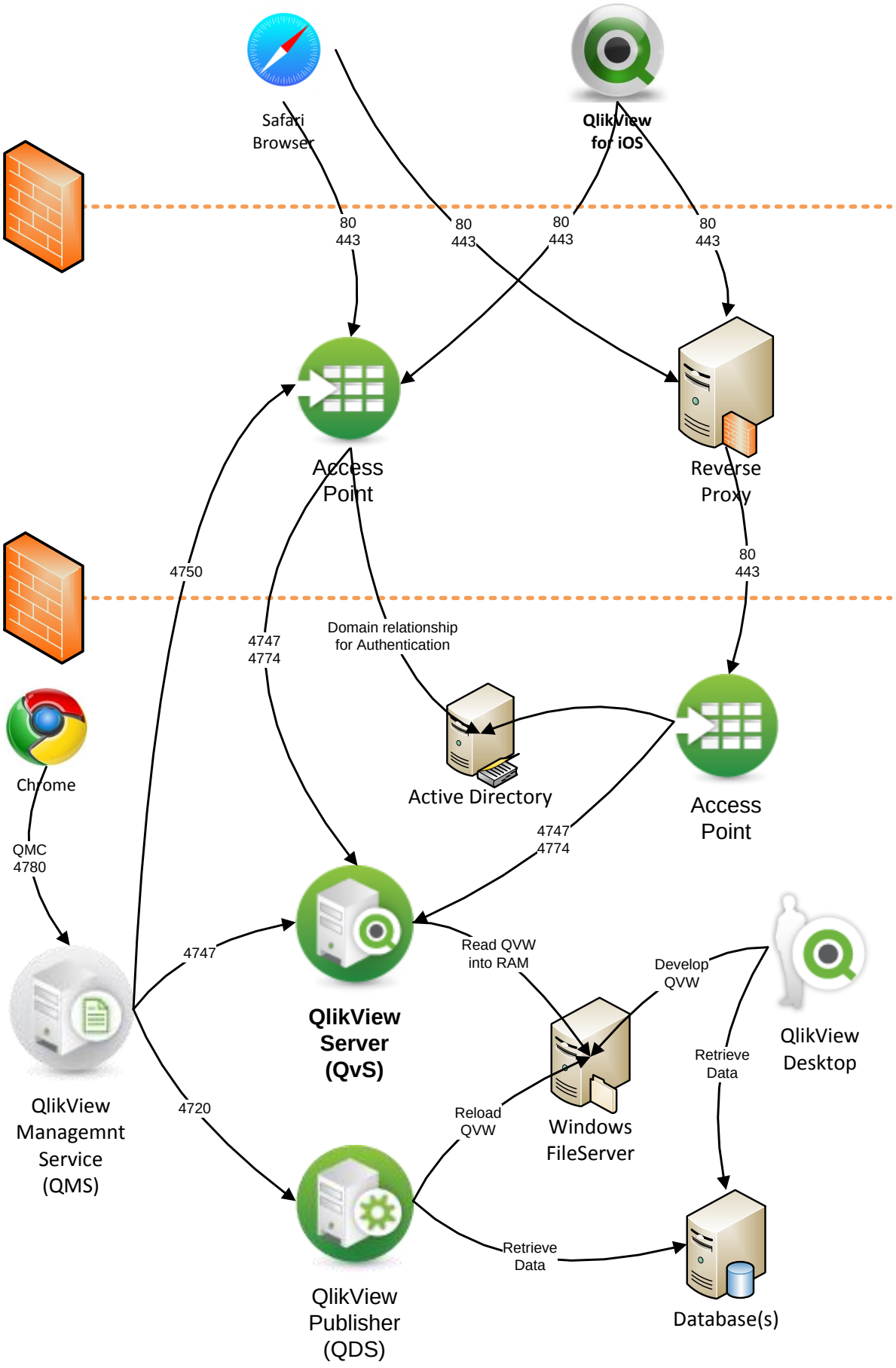
Users typically interact with QlikView documents using a Javascript and HTML5 enabled browser such as Apple Safari or Google Chrome or **Good Access**. Other clients also exist: eg ActiveX client for Microsoft Internet Explorer, and a client-server connection from the QlikView Desktop directly to the QlikView Server or tunneled via the QlikView AccessPoint Portal.
Several authentication mechanisms may be supported by the AccessPoint website, and connectivity is typically simply HTTP on 80/tcp however HTTPS is also supported.

The **QlikView for iOS** client may be used in place of a browser (Safari on iOS, Chrome on Android) if the QlikView AccessPoint Portal is hosted in DMZ or is accessible via VPN. This client also provides the ability to access images of QlikView content while disconnected from the QlikView AccessPoint portal.

QlikView for Good may be downloaded from the Apple AppStore, and provides the same functionality as the **QlikView for iOS** client above but leverages the secure connectivity [via **Good Proxy**], secure storage and remote wipe capabilities of the Good Dynamics platform.

Qlik Community

The Qlik Community https://community.qlik.com/welcome contains discussion forums, documentation and links to Support and Downloads. It is an extremely useful source of guidance from other Qlik customers.


Safari
Browser
QlikView
for iOS
80
443
80
443
80
443
80
443
Access
Point
Reverse
Proxy
4750
80
443
4747
4774
Domain relationship
for Authentication
Chrome
Active Directory
Access
Point
QMC
4780
4747
4774
4747
Read QVW
into RAM
Develop
QVW
QlikView
Server
(QvS)
QlikView
Desktop
Retrieve
Data
QlikView
Managemnt
Service
(QMS)
4720
Reload
QVW
Windows
FileServer
Retrieve
Data
QlikView
Publisher
(QDS)
Database(s)

Integration

When considering using the **QlikView for Good** application, first ensure that **Good Access** has successful connectivity to the QlikView AccessPoint website.

1) Connectivity
   a) Can you successfully browse to QlikView AccessPoint from a desktop Browser within the LAN?
   b) Do firewalls between the **Good Proxy** and the QlikView AccessPoint website permit browser traffic?
   c) Is the Server address and port for QlikView AccessPoint whitelisted on the **Good Proxy**?

2) SSL Considerations
   a) Does **QlikView AccessPoint** get delivered over HTTPS using a Self-Signed Certificate? These will cause the browser to prompt the user whether the SSL Connection is acceptable. The **QlikView for Good** application does not prompt for such a certificate error and will simply fail the connection request. See also https://blog.httpwatch.com/2013/12/12/five-tips-for-using-self-signed-ssl-certificates-with-ios/
   b) Does QlikView AccessPoint get delivered over HTTPS using an SSL certificate from a private Certificate Authority (CA)?
   This certificate chain will not be trusted on the mobile device unless the CA has been propagated to the Certificate Store on the mobile device. This can be performed using GC, but it is recommended that if SSL is required [even though the traffic from the Good client to the **Good Proxy** is already encrypted] then the SSL Certificate should be acquired from a publically trusted CA. See also https://support.apple.com/en-us/HT204132

3) Authentication
   a) What authentication mechanisms are required by QlikView AccessPoint?
   Good Access is capable of more authentication mechanisms than **QlikView for Good**.

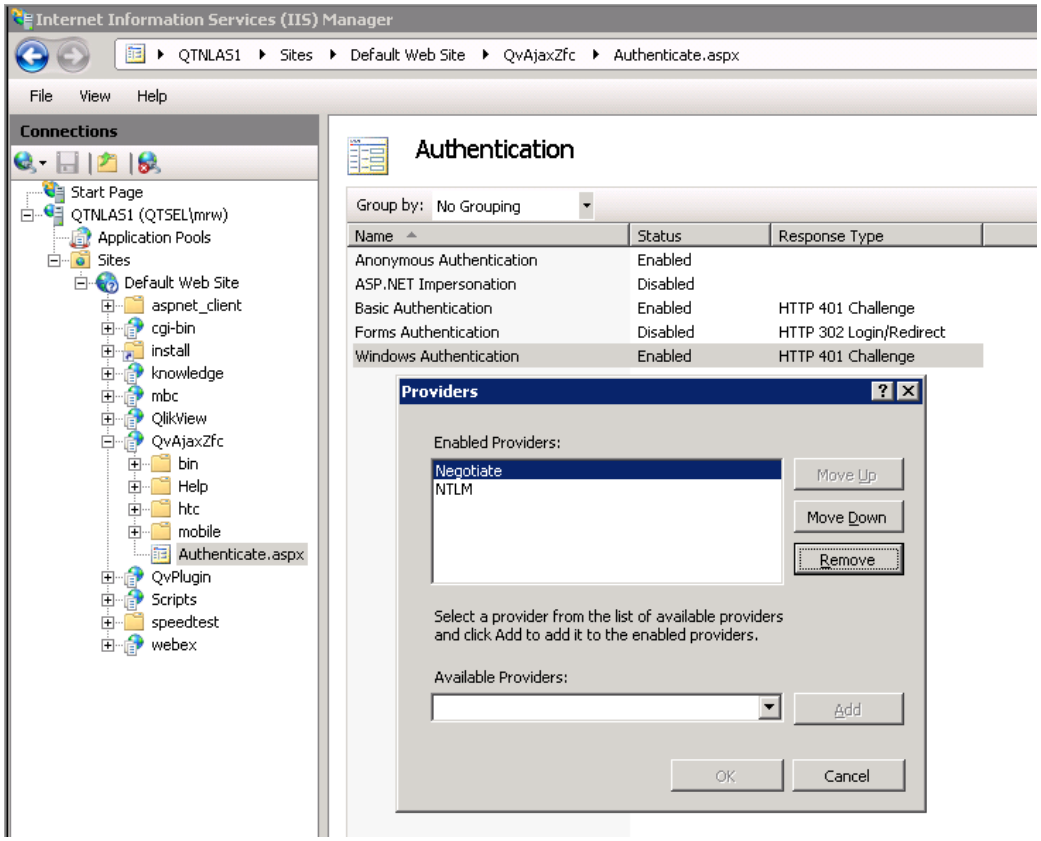
   If the **Good Proxy** is configured with Kerberos Delegation rights then seamless Kerberos Authentication to AccessPoint may be possible. Refer Good Dynamics Kerberos Constrained Delegation (KCD) https://community.good.com/docs/DOC-2716

   Good Access and **QlikView for Good** can also utilize Forms Authentication, and support NTLM and HTTP Basic authentication.

   Several Qlikiew AccessPoint webservers may be necessary to support multiple forms of authentication (eg Forms and Windows Integrated) but resolving to the same QlikView Server(s).

b) When using IIS for delivery of QlikView AccessPoint, the default authentication properties are incorrect. The QlikView Server installation program will correctly permit HTTP Anonymous access to “/QlikView” but requires Windows Integrated Authentication for the whole of “/QvAJAXZfc” which is unnecessarily broad. The scope of authentication may be reduced to only “/QvAJAXZfc/Authenticate.aspx”.

QlikView for Good does not support the *Negotiate* provider for *Windows Authentication*. This must be removed from the authentication scope in IIS.



i) Invoke IIS Manager
ii) Navigate to the Web site where the AccessPoint content has been deployed
iii) Select “QlikView” virtual folder (left navigation frame)
   (1) Open the Authentication properties (right “Features View” frame)
   (2) Enable “Anonymous Authentication”,
   Disable “Windows Authentication” and any other authentication methods.
iv) Select “QvAJAXZfc” virtual folder (left navigation frame)
   (1) Open the Authentication properties (right “Features View” frame)
   (2) Enable Anonymous,
   Disable Windows Authentication and any other authentication methods.
v) At the bottom (right frame), Click “Content View”
   (1) Navigate to “QvAJAXZfc/Authenticate.aspx”, right-click on it and select “Switch to Feature View”
   (2) Open the Authentication properties (right “Features View” frame)

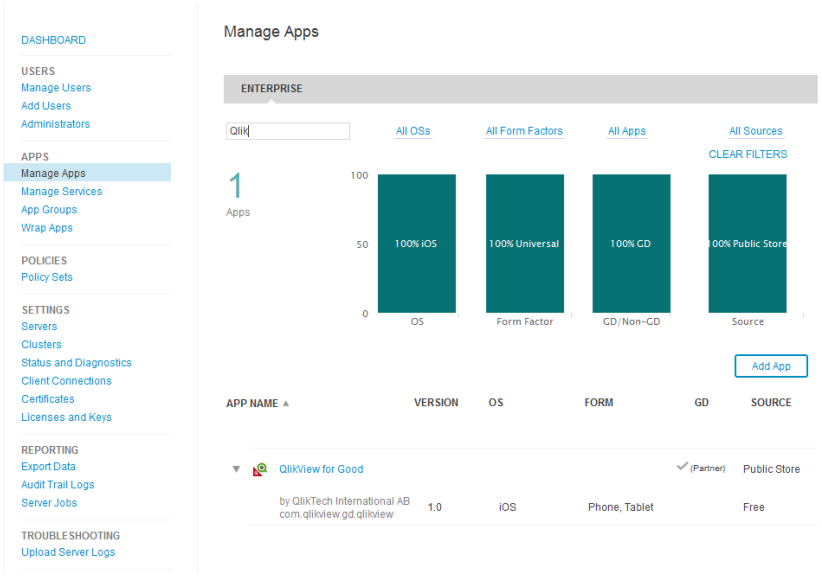
(3) Enable “Anonymous Authentication” if authentication is optional (the “Login” option in QMC WebServer properties) or if using QlikView Forms authentication.
(4) Enable “Windows Authentication” if authentication should be performed using Active Directory or local Windows identities
(a) Right-click on “Windows Authentication”, select “Providers”
(b) **Remove the *Negotiate* provider**, leaving only the *NTLM* Provider

vi) Verify that under QvAjaxZfc\htc only “Anonymous Authentication” is enabled.
vii) Invoke “iisreset” at Command-Line to restart IIS and activate these changes.

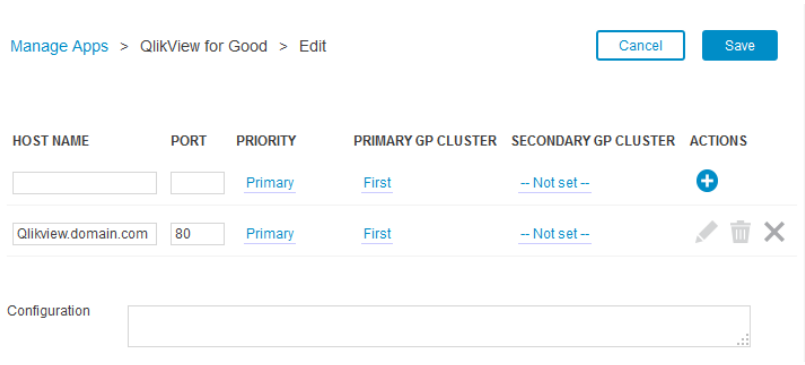
Only after ensuring that **Good Access** can interact with QlikView AccessPoint, and if you require additional Offline functionality then install and test **QlikView for Good**.

See https://itunes.apple.com/en/app/qlikview-for-good/id880582606

4) Ensure that **QlikView for Good** is available in your list of applications
a) Logon to the **Good Console**
b) Click the **Manage Apps** link (or Manage Applications for versions prior to v1.9) in the **Apps** menu on the left hand side.
c) Search for **QlikView for Good** in the search box in the page displayed.
d) If the application is not present, then please request it from the Marketplace in **Good Community** https://community.good.com/gd-app-details.jspa?ID=138193661

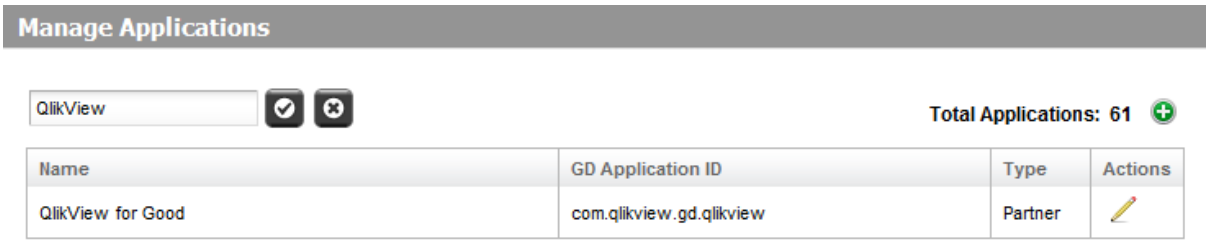


5) Setup the QlikView AccessPoint servers in **Good Console**
a) In v1.10 this is done by
i) Clicking on the application, name, then
ii) select **GOOD DYNAMICS** tab at the top
iii) In the Servers section click Edit
iv) Add the FQDN of the QlikView AccessPoint server, the port (typically 80/443) and click the button to the right to add the server
v) Click Save to save the changes



b) In versions prior to v1.10 this is done by

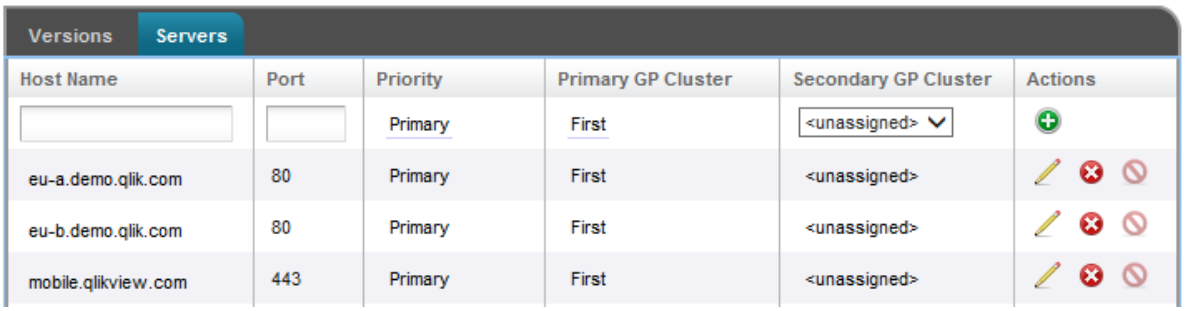
i) clicking on the pencil icon to edit the application



ii) select the **SERVERS** tab at the top

iii) Add the FQDN of the server, the port and click the button to the right to add the serve

iv) Click Save to save the changes



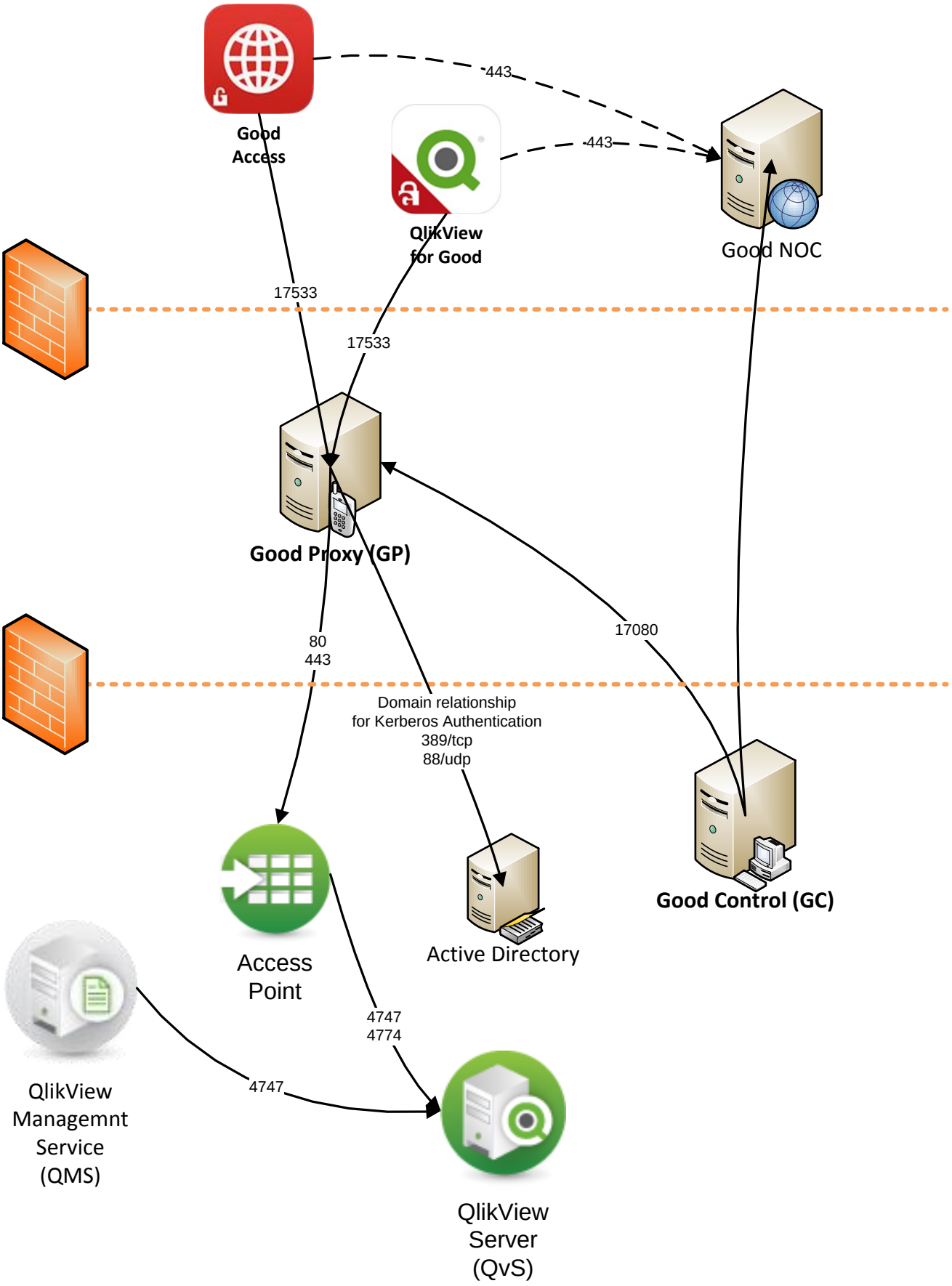
c) The **Good Proxy** host needs to be able to resolve the FQDN of the QlikView AccessPoint server and be able to route traffic on the specified port. Note you can add several different QlikView AccessPoint instances at this level and assign them a Primary, Secondary or Tertiary status

6) Publish the Application to the required Users

a) Click on **App Groups** link (v1.9 and higher) or **Manage Applications** link under Apps on the left hand side.

b) Identify or create a new application group then assign **Qlikview for Good** to the application group.

c) Associate the required users with the application group. The users should now be able to activate the **Qlikview for Good** application on their mobile devices.


Good Access
443
443
QlikView for Good
Good NOC
17533
17533
Good Proxy (GP)
80
443
17080
Domain relationship
for Kerberos Authentication
389/tcp
88/udp
Access Point
Active Directory
Good Control (GC)
4747
4774
4747
QlikView Managemnt Service (QMS)
QlikView Server (QvS)

Troubleshooting

1) I can successfully access Google and even the QlikView Demo site https://mobile.qlikview.com/ using **Good Access**, but I cannot access our QlikView AccessPoint.
   a) Is QlikView AccessPoint accessible from within the LAN using a desktop browser?
   b) Has the QlikView AccessPoint webserver been *WhiteListed* in **Good Control**?
   c) Are firewalls between **Good Proxy** and QlikView AccessPoint webserver configured to permit browser traffic to the QlikView AccessPoint website?
   d) Did you incorrectly record the full QlikView AccessPoint URL http://webserverHost/qlikview in **QlikView for Good**, when you only should only record the host http://webServerHost
2) I can access QlikView AccessPoint using **Good Access** but not using the QlikView Mobile Client for iOS
   a) QlikView Mobile for iOS is not supported on Good infrastructure.
   This client works only when the AccessPoint website is directly accessible.
   You should download **QlikView for Good** from the AppStore if you need Offline access to QlikView content.
   b) **QlikView for Good** requires refinements to the default Authentication settings in IIS
3) I can access QlikView AccessPoint using **Good Access** but not using the **QlikView for Good**
   a) Are you prompted for Kerberos Authentication using **Good Access**? This may indicate that the Negotiate provider is still enabled in IIS, and must be removed before **QlikView for Good** can authenticate.
   b) Do you get prompted to accept any SSL Certificate details when using **Good Access**? These errors need to be addressed so that interaction is seamless otherwise **QlikView for Good** will not work.
   c) Is QlikView AccessPoint integrated with any special authentication system, causing it to redirect to another webpage which prompts for your credentials? You may have to use **Good Access**.
4) Why can't I synchronize QlikView content to my mobile device?
   a) Is the additional **QlikView Offline Service** installed on the WebServer?
   b) Has the "Offline" attribute [with value "True"] been added to the User Document in QMC? Refer s3 "Preparing for Offline Mode" in "QlikView Mobile Client Reference Manual".
   c) Do you have any bookmarks defined within the Document? One of the first steps when preparing to sync content is to select a Bookmark which refines what data will be synced.
5) I see a document in QlikView AccessPoint when using **Good Access** but it isn't present when using **QlikView for Good**
   a) Is the attribute "Invisible" present on the User Document in QMC, with value "True"?
6) Does **QlikView for Good** support my company's authentication system?
   a) Any customized authentication required for interaction with QlikView AccessPoint may require that you use the **Good Access** browser rather than **QlikView for Good**.
7) I have no idea what is going on
   a) Start by reading the "QlikView Mobile Client – Quick Reference Manual" downloadable from the Qlik Download site http://eu-b.demo.qlik.com/download/ eg v11.20sr11 document https://d1cf4w4kkla6tb.cloudfront.net/qlikview/11.20/12852/QlikView%20Mobile%20Client%20Reference%20Manual_ENG.pdf
   b) Further study the "QlikView Server Reference Manual" also downloadable from Qlik.
   c) Contact your Qlik or Good Account Manager to engage a Professional Services consultant for further assistance.