



User Manual

Get Console Private Server

Version: 1.6.1

Date: 19 March 2014

CONTENTS

Revision History	3
What Is Get Console Private Server?	3
Get Console App	4
AIRCONSOLE Adaptor	4
Get Console Server	4
Obtaining the Private Server Software	5
Virtual Appliance Requirements.....	6
Firewall Port Requirements.....	6
Common Deployment Architecture (SELF HOSTED)	8
Common Deployment Architecture (AMAZON EC2 HOSTED)	9
Installing VMWare Appliance	10
Installing with VMWare Server.....	11
Installing with VMWare vSphere.....	11
Initial Network Configuration	14
Private Server Licensing	14
How licensing works	14
Licence activation procedure	15
Obtaining License Keys.....	15
Activating Private Server License	16
Private Server Web Administration	17
Home Page	17
Network Settings	17
Files Section	18
Accounts	20
SSL Certificate	20
Generate Certificate Signing Request.....	21
Obtaining SSL Certificate	23
Upload SSL Certificate to Private Server.....	24
Updating the Private Server Software	25

Software Updates 25

Automatic Upgrades 26

Manual Updates..... 27

Configuring AirConsole Adaptor to use Private Server 28

Configuring iOS Device Get Console App to use Private Server.... 29

ACcessing Remote Terminals..... 31

SCRIPT MANAGER 32

Troubleshooting Connectivity to Private Server 34

 General Connectivity Issues 34

 Server Not Recognized by License Server 34

 Incorrect Username or Password 34

 License Issues 35

REVISION HISTORY

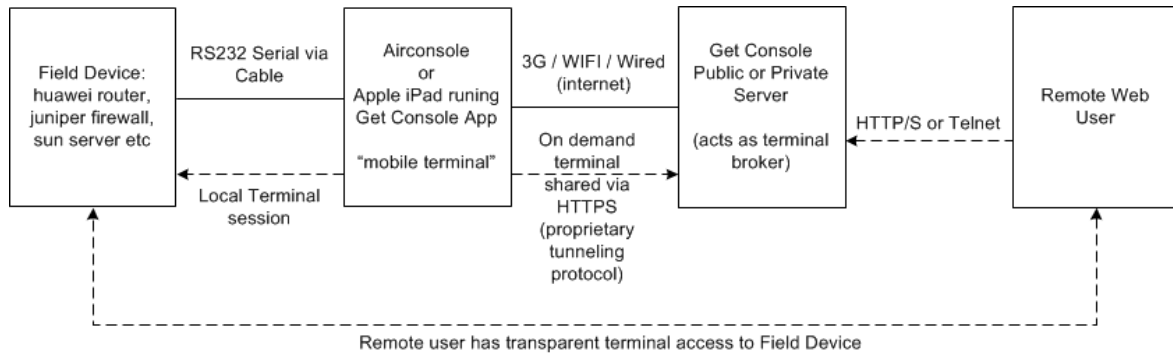
Revision	Date	Description	Author
1.04	5 May 2011	First Release	SH / RP
1.20	30 August 2011	Second Release for Private Server v1.2	SH / RP
1.5.1	4 December 2013	Update for Private Server version 1.5	SH / EH
1.6	18 Mar 2014	Update for Private Server version 1.6	SH

WHAT IS GET CONSOLE PRIVATE SERVER?

There are 2 Components to the Get Console solution

- 1) Clients– such as the Airconsole adaptor, or the Get Console App which runs on Apple iPads and iPhones
- 2) The Get Console Server which can be either the Public or Private version

The below drawing summarizes the components of Get Console



GET CONSOLE APP

The Get Console app provides iPads and iPhones with terminal connectivity via **Serial, Telnet** or **SSH** to IT equipment (for example, a Cisco router or a Linux Server). This allows a field engineer to configure such IT equipment in the field using the apps intuitive terminal window. The app can then optionally act as a terminal server to **share** its Serial/Telnet/SSH sessions with remote users via a Get Console Server (Public or Private).

The app is designed primarily to be a mobile terminal – it enables field engineers connect to and configure network devices and servers via these devices' serial console ports (or SSH/Telnet server), and then, if required, use the Apple 3G or WIFI connection to share the terminal window.

AIRCONSOLE ADAPTOR

The Airconsole Adaptor is a small battery or external powered Serial over IP (WIFI or Ethernet) adaptor that allows transparent access to RS232 serial ports over IP. Airconsole (firmware 2.1 and greater) has the ability to dynamically tunnel its serial port to the cloud based Get Console Private Server (while concurrently being accessible to local users terminal client).

This allows the Airconsole to be used as both a personal Serial-IP adaptor for engineers to configure Industrial or IT equipment in the field, or optionally to be used as a more permanent Out-of-Band serial terminal server to manage remote serial equipment via the Private Server.

Using Private Server allows for multiple Airconsole adaptors in different remote locations to be aggregated, controlled and accessed via a single dashboard.

GET CONSOLE SERVER

There are 2 versions of the Get Console Server

- 1) The publicly available Get Console Servers hosted at the website www.get-console.com
- 2) The private version, which is hosted on a customers own network, and secured by their own network security policy (the subject of this user manual).

Both versions of the Get Console Server acts as a connection broker and proxy between the Airconsole or Apple iPad/iPhone terminal session and the remote users web browser, allowing the remote web user to control the terminal session connected to the Apple iPad/iPhone or Airconsole.

Public versions of the Server are hosted in US, UK and New Zealand. These can be used at no charge by any registered purchasers of the Get Console App to allow any remote PC to access the terminal session via the public website www.get-console.com. The performance of the end to end terminal varies greatly on the

current load of the server and the latency of both the Apple device and the Remote PC users from the selected public server. The public server is also limited in that it does not have the terminal scripting, file management or logging features of the Private server.

The Get Console Private Server extends the functionality of the Get Console solution by allowing end users or corporations to deploy their own privately hosted version of the Get Console public server component. This has the following benefits:

- Aggregation of all remote iPads/iPhones and/or Airconsole devices in the field into a single management window. This lets NOC or Colo operators remotely control and operate both fixed (Airconsole) or roaming (Get Console) serial port connections to remote field equipment
- Advanced integrated terminal scripting – access the terminal of remote devices directly, or easily create powerful scripts and push them down to remote devices for controlled execution.
- Fast Remote Access: The end to end performance of the remote control terminal session is fast and smooth. The http based communication protocol with Airconsole is significantly optimized when using the Private Server vs the Public Servers.
- Flexible Access - the Remote user can use either the Private Servers built in Web Terminal, or any Telnet client of their choosing (such as SecureCRT, or puTTY) to access remote Airconsole and Get Console app terminal screens.
- Easy to Use: As the Private Server displays all currently available sessions and the name of the mobile terminal associated (generally the field engineers name). The field engineer does not need to pass the session code number to the remote PC user, as the remote PC user can see all the sessions and quickly identify the session he wants to connect to.
- Increased Security, as the Private Server and Remote PC user are generally located behind the corporate firewall, so no potentially sensitive field device configurations or data is transmitted through or stored on the public Get Console servers. In addition, the Private Server can install a valid corporate SSL certificate to allow the Apple device to Private Server connection to use SSL encryption.
- Private Server (1.6+) features a fully integrated terminal scripting engine that allows for the creation, editing, upload, download and remote execution of Expect style scripts
- Keep log files of all field terminal sessions and upload them automatically for audit trail and troubleshooting

OBTAINING THE PRIVATE SERVER SOFTWARE

The Get Console Private Server software is available in a number of ways

- 1) Customer downloads the VMWare Virtual Appliance and hosts it on their own internal VMWare infrastructure (see below)
- 2) Customer deploys the Amazon Machine Image version of Private Server into their own existing Amazon EC2 Cloud (see <https://aws.amazon.com/marketplace/pp/B00J0I7YFW>)
- 3) Cloudstore (our company) hosts the customers Private Server for them in our private Amazon EC2 Cloud. This is purchased in our webstore at <http://www.get-console.com/shop/en/15-hosted-private-server-solutions>

In all deployment models, the Private Server software is free to deploy or for VMWare the VM download is available from the www.get-console.com/private-server website. The download file is packaged as either an OVF (Open Virtualization Format) package, or a VMWare vmx/vmdk package.

While the download is free, the Server will not work with Apple iOS devices or Airconsole until it is licensed (see licensing section below).

Get Console offers support for VMWare Server 2.0 or vSphere 4.0 and above installation of the vmx/vmdk package. The OVF format package is supplied for other non-VMWare virtualization hypervisors, however it has not been tested on other hypervisors.

If you are running VMWare we recommend downloading the VMX/VMDK zip file and install as per the instructions in the later sections.

For either self hosted or cloudstore hosted Amazon deployments, the installation is automatic and once complete an email describing access will be sent to the customers provided email address. The following sections are only applicable to the VMWare Virtual Machine version.

VIRTUAL APPLIANCE REQUIREMENTS

These requirements are for customers hosting their own VMWare virtual machine. For Amazon deployments no interaction is required - please skip to the licensing section below.

The Get Console Private Server Appliance has the following minimum specification:

Operating System: Centos 5.5 **64 bit**
 CPU: 1 Processor
 Memory: 1 GB
 HDD: 5 GB

VMWare Hardware Version Support Required: **version 7**

As the Get Console Private Server is a 64 bit "Guest OS" appliance. It will only run on a 32 bit host operating system if the underlying CPU of the physical host machine is 64 bit capable. See the following table from vmware.com to understand compatibility.

	Host OS	32-Bit Guest OS	64-bit Guest OS (ie Get Console)
32-Bit CPU	32-Bit Host OS	Supported	Unsupported
	64-Bit Host OS	Unsupported	Unsupported
64-Bit CPU	32-Bit Host OS	Supported	Supported
	64-Bit Host OS	Supported	Supported

Private Server (v1.3 and later) can also integrate with an existing corporate trouble ticket system. If this feature is enabled, the Private Server will require its own email account on the corporate mail server, and rights on this server to send mail via SMTP (port25) and be able to POP its mail account (port 110).

FIREWALL PORT REQUIREMENTS

The following Table describes the ports used by the Private Server. These ports will need to be open to the Private Server from any intervening firewall. For Amazon deployments these firewall rules are added to the Security Group that is automatically bound to the Private Server instance (VM).

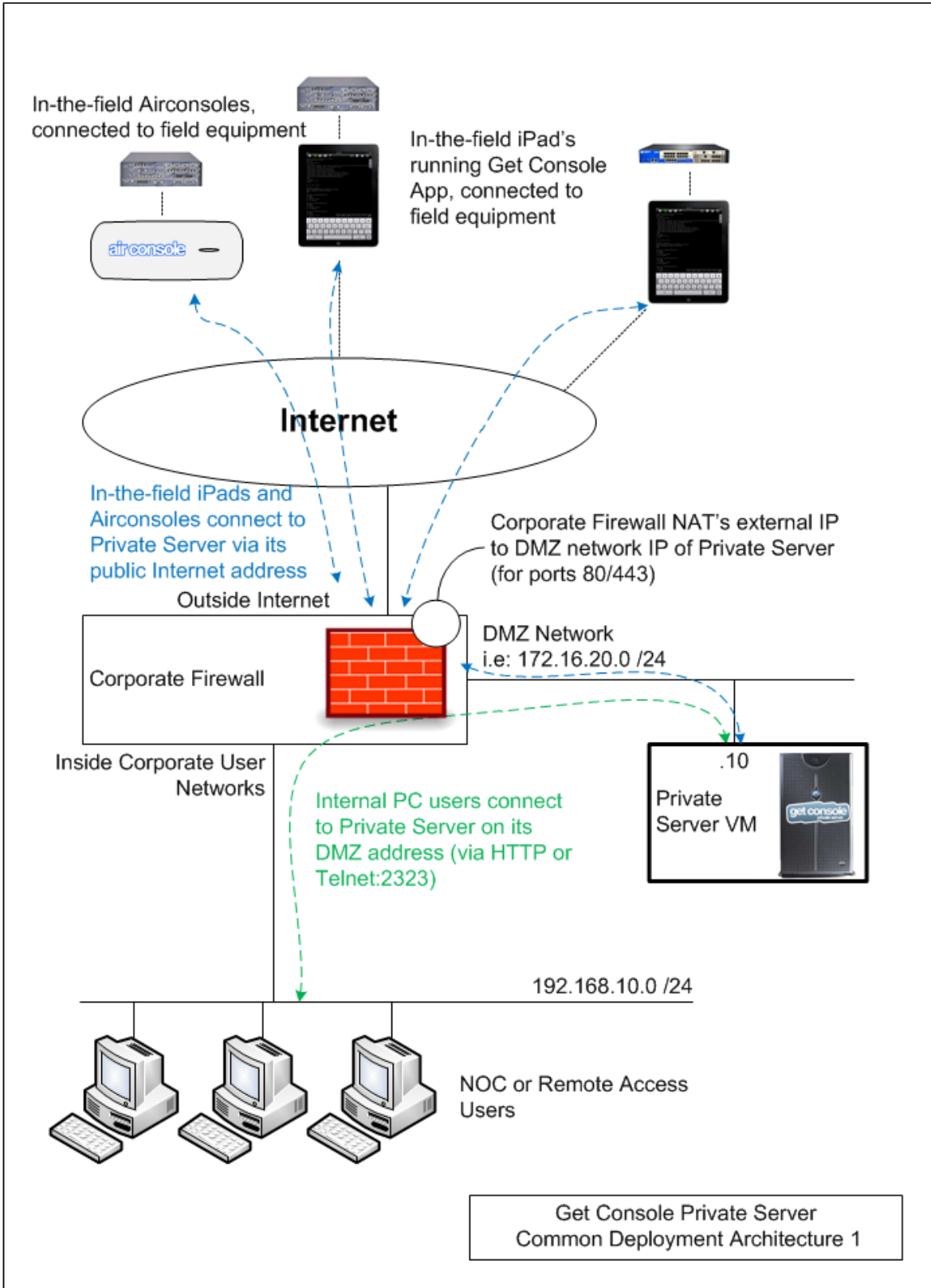
TCP Port	Description	Used For
80 (inbound/outbound)	HTTP	From iPhone/iPad to Private Server tunnelling serial session to Private Server

		From Remote PC user to Private Server for accessing the admin and web-terminal function
443 (inbound/outbound)	HTTPS	(Where SSL certificate has been installed, and the secure connection is selected in the iPad / iPhone app settings) From iPhone/iPad to Private Server tunnelling serial session to Private Server From Remote PC user to Private Server for accessing the admin and web-terminal function This port is also used outbound from the Private Server to check the www.get-console.com website for software updates.
2323 (inbound)	Telnet	From NOC/Remote User PC to Private Server (if using third party telnet client (ie SecureCRT/Putty)
22 (inbound)	SSH	(optional) Used for remote management of Get Console Private Server itself. Enable this port if requested by Cloudstore support for remote maintenance on your Private Server
25 (outbound)	SMTP	(optional) used between Private Server and user defined mail gateway – used for sending updates to troubletickets / service requests back to existing corporate ticket service desk software
110 (outbound)	POP	(optional) used from Private Server to download its troubletickets from its user provided mailbox on the Corporate email system

In addition to the above TCP port requirements, a general requirement of Private Server licensing is the provision of Private server on a Static IP address. The IP address can be either public or private, however in order to successfully license Private Server it cannot dynamically change.

COMMON DEPLOYMENT ARCHITECTURE (SELF HOSTED)

The below drawing describes the most common high level network design for deploying self hosted Private Server.



While not the only method, this design allows the Private Server to be securely placed where remote Internet connected iPads and iPhones can reach it, while also allowing secure access from internal users.

Other alternatives include forcing internet connected remote iPads and iPhones to use the iPad/iPhones built in Cisco VPN client to build a IPSEC VPN tunnel to the Corporate Firewall (VPN Concentrator) and then launch the Get Console session sharing connection to the Private Server. This alternative alleviates the need for NAT, and also means Private Servers hosted behind dynamic public IP addresses can be used via a static internal private IP address.

COMMON DEPLOYMENT ARCHITECTURE (AMAZON EC2 HOSTED)

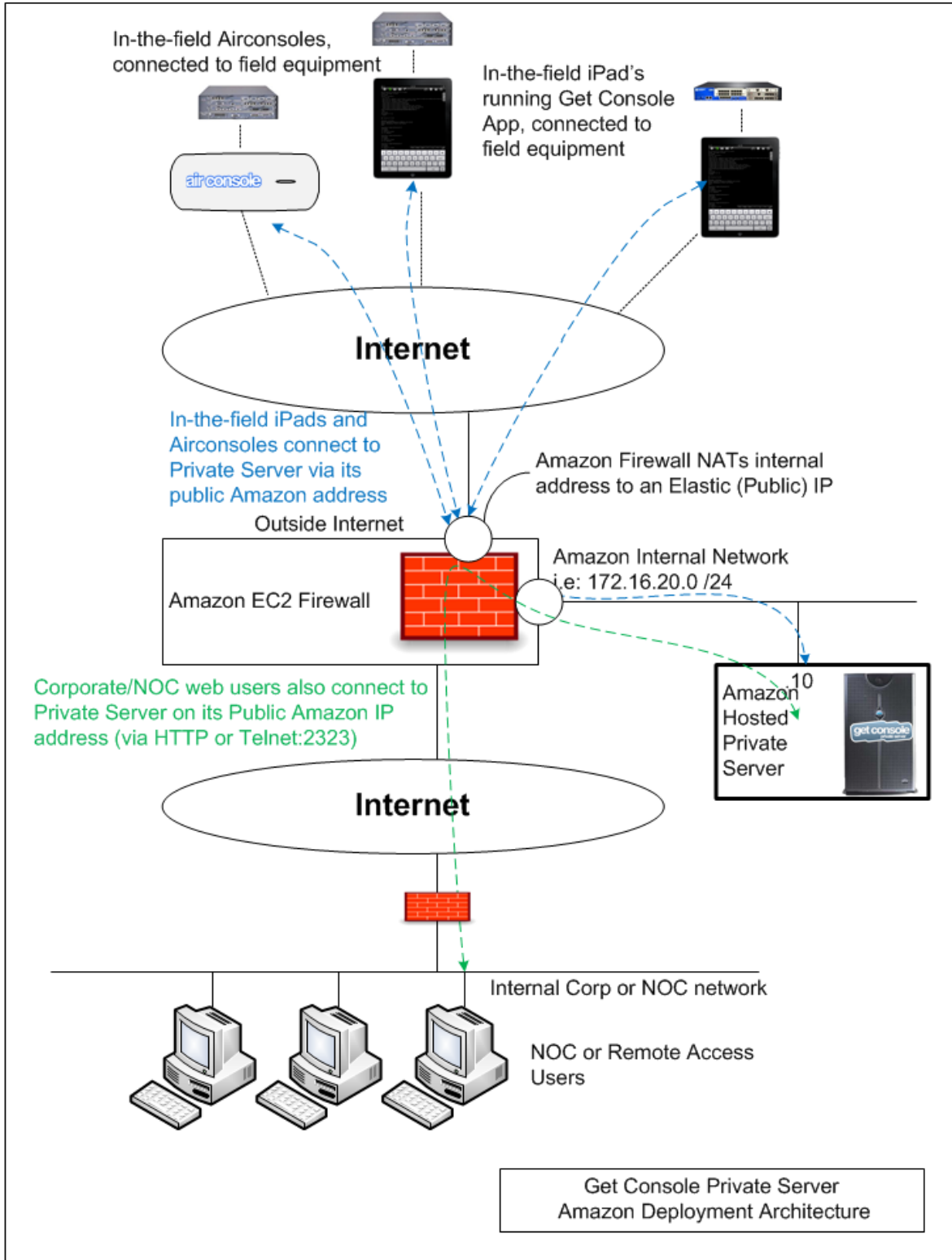
The below drawing describes the high level network design for Amazon deployed Private Server.

Using Amazon deployment, both the remote serial device connections (coming from Airconsole's or iPads/iPhones running Get Console app) and web users access Private Server via the Amazon public IP assigned to the Private Server at build time.

We recommend using an Amazon "Elastic" IP, so that the public IP address of the Private Server does not change after any prolonged downtime.

The assigned Amazon security group (firewall ruleset) for the Private Server instance can be customized to restrict access to just the IP networks needed through the Amazon console.

If additional security is required other than the Amazon security group then the customer can deploy other third party firewall virtual appliances in front of their Private Server instance. These 3rd party firewall instances (VMs) are available from the Amazon Marketplace.



INSTALLING VMWARE APPLIANCE

This section provides instructions for installing the Get Console Private Server on either VMWare Server 2.0 (free) (Vmx/VMDK package), or on a VMWare vSphere Cluster (OVF package). Other VMWare platforms should follow the VMWare Server instructions. Non VMWare platforms should work however are not

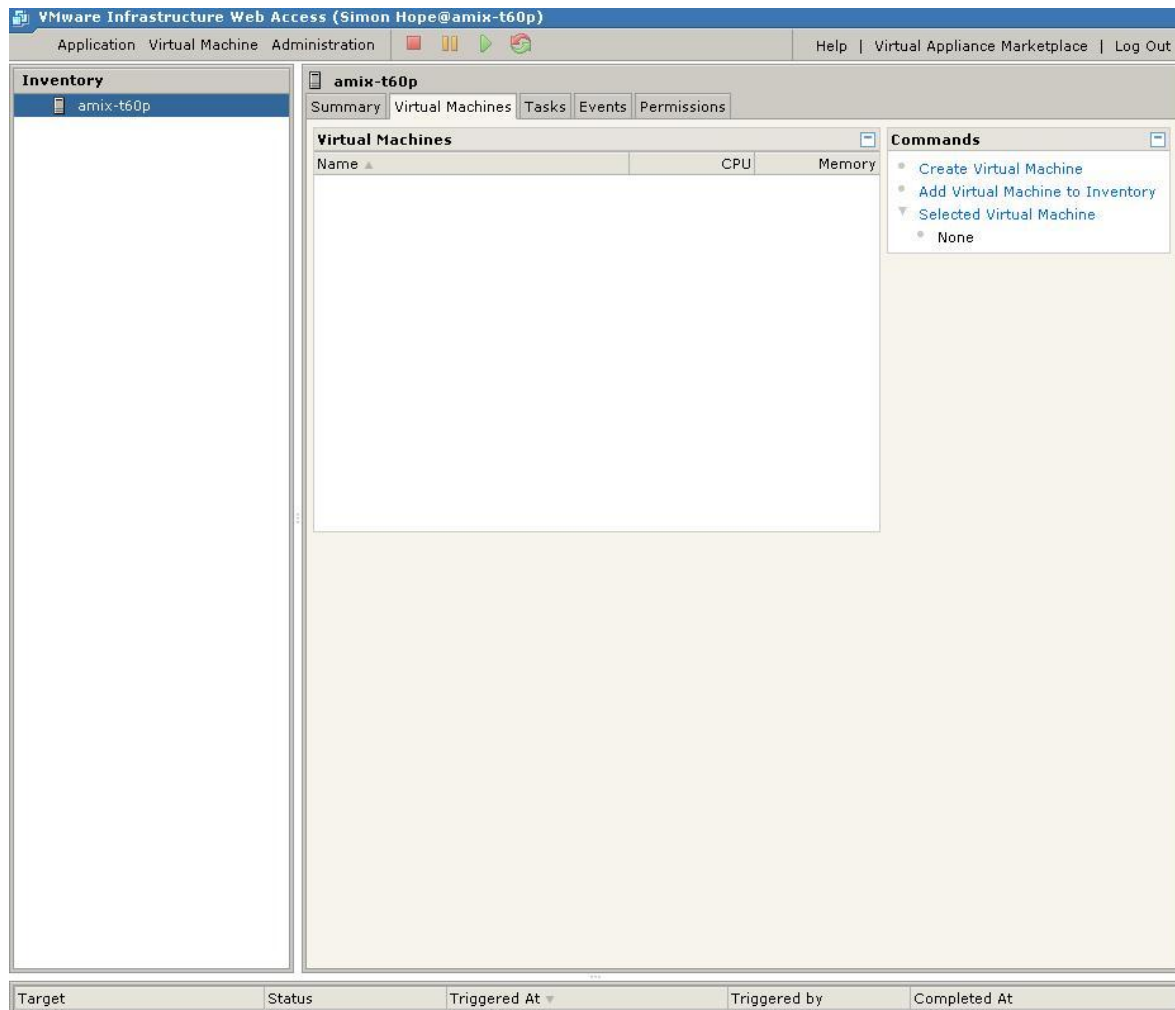
officially supported – please see the community forum at www.get-console.com/forum for community support on non VMWare hypervisors.

INSTALLING WITH VMWARE SERVER

To install the Get Console Private Server software in VMWare Server (version 2.0 or later):

Download the latest vmx/vmdk package from the Get Console website. Unzip into your virtual machines directory onto a datastore location of your VMWare Server.

Launch VMWare Server. Select Virtual Machines tab. Then select Add Virtual Machine to Inventory.



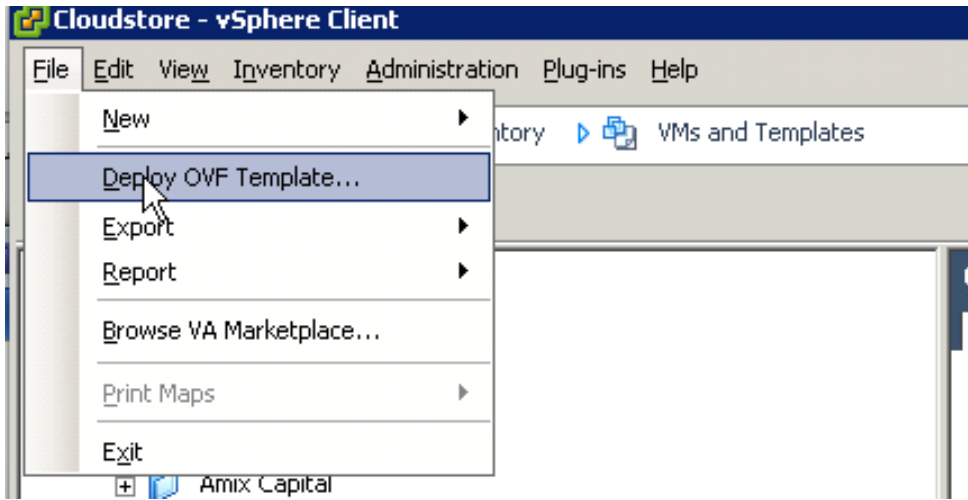
Select the .vmx file from the unzipped package from the get console web site and click open. The appliance will install.

The VM status must display a Success status at the bottom of this page to have been correctly loaded.

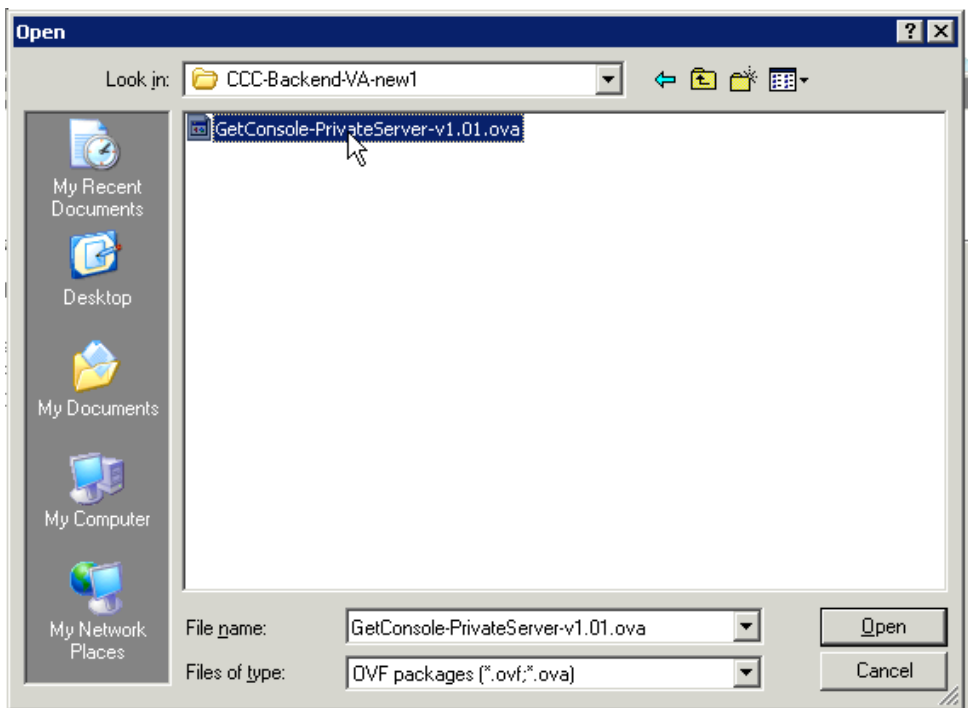
Select the play button to start the appliance. Follow the Initial Network Configuration Instructions and Web administration sections below to complete the installation.

INSTALLING WITH VMWARE VSPHERE

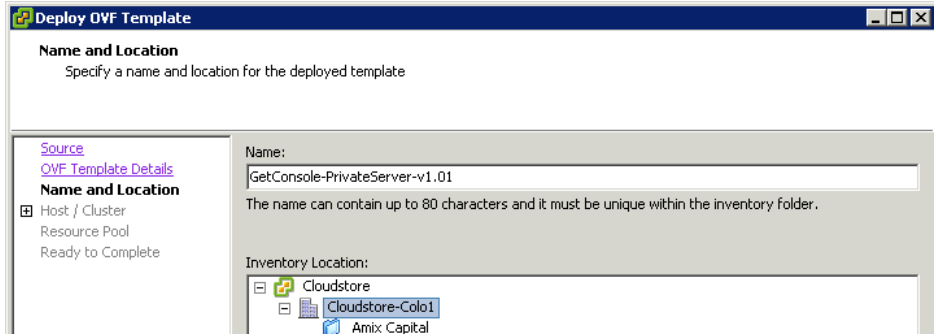
To setup the Private Server with vSphere, download the image to a datastore repository visible to the vSphere server(s). Either the VMX/VMDK or OVF package will work with vSphere. The instructions below use the OVF package.



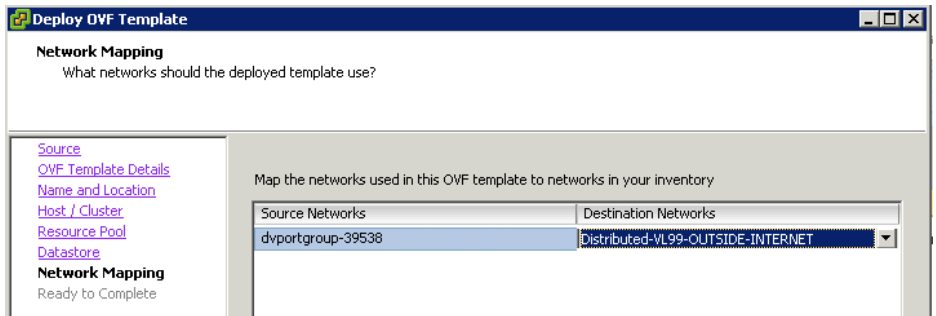
Select the .OVA file from the downloaded package (for method to install .vmx use the New Virtual Machine wizard using the vmx/vmdk as the existing VM disk)



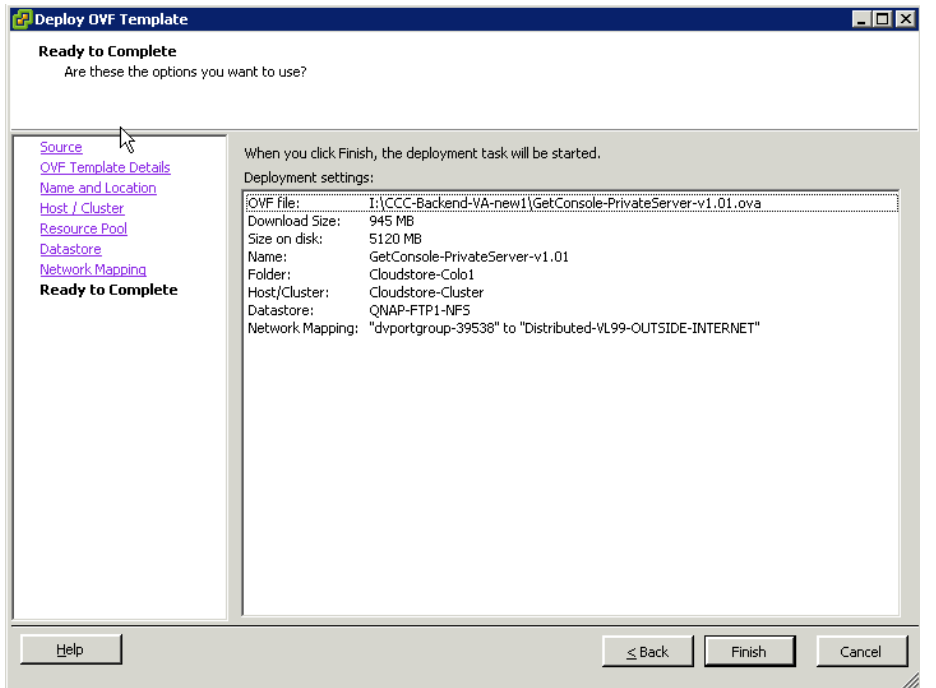
Follow "Deploy OVF Template" Wizard



For the network settings – map the network port of the OVF template to your desired VMWare NIC or VLAN. In this example case as the appliance will have a public IP address we have mapped to an external VLAN. If mapping to an internal or DMZ privately addressed VLAN or NIC, then for your server to be reachable from internet connected Apple iOS devices, the required NAT translations on your external firewall for TCP ports 80 and/or 443 to the Private Server will be required (see Common Deployment Architecture section).



Prior to deploying, the Wizard summarizes the options selected



Post installation, start the Virtual Appliance with the power on button, then open the web console for the virtual machine to complete the initial network configuration steps as described in the next section.

INITIAL NETWORK CONFIGURATION

After deciding on the deployment design, the first task in configuring the Private Server is to set the IP address and default gateway. This is done by following the steps below:

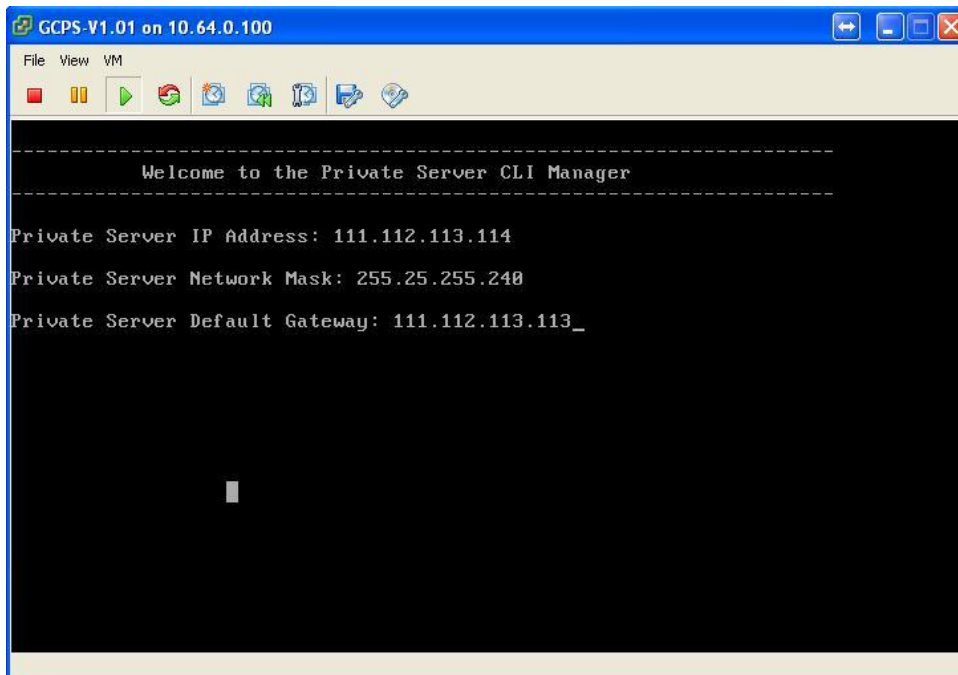
Once the Private Server is available in VMWare and has been booted, launch the Virtual machine Web Console. A Centos console will be presented with a login and password prompt.

The default username and password are

USERNAME: **webadmin**

PASSWORD: **w3badm1n!**

As the virtual appliance comes up with no network configuration, (apart from being mapped to the VLAN or Virtual NIC that was allocated during the OVF or VMX installation), this CLI wizard is used to set the initial network configuration. As DHCP is disabled, this initial network configuration must be provided via the VMWare web console with CLI interface:



NOTE: the above IP address details in the graphic are examples only. Use addressing as per your deployment design.

After completing this script, the Private Server will start with the configured IP settings. After this step all remaining configuration can be completed via the web interface by navigating to:

[http://\[ip-address-given-to-server\]/](http://[ip-address-given-to-server]/)

PRIVATE SERVER LICENSING

HOW LICENSING WORKS

The Get-Console Private Server is freely accessible to download from the web site, however each unique iOS device or Airconsole wishing to connect to the Private Server uses a Client Access License (CAL) that must be purchased in advance of use from the Get-Console.com shop. Airconsole Pro and XL units ship with a redemption card for 2 Private Server licenses.

The CAL is enforced when the Apple iOS device or Airconsole tries to connect to the Private Server for the first time. On first connection, the Apple iOS device / Airconsole will initially make a check with our license server to see if the Private Server as configured has free licenses available, and if so will store the iOS device UDID (or Airconsole MAC address) against that Private Server and decrement the number of free licenses available. The Private Server owner can delete unwanted UDIDs consuming CAL's by contacting us at support@get-console.com (a self service web portal for this purpose will become available later in the year).

LICENCE ACTIVATION PROCEDURE

After purchasing licenses from the www.get-console.com/shop, the purchaser can obtain their license key and then apply it to their installed server.

There are 2 parts to licensing Get Console Server.

- 1) Obtaining License Key from www.get-console.com/redeem
- 2) Activating License against particular server at www.get-console.com/activation

OBTAINING LICENSE KEYS

After purchasing Private Server licenses, or Airconsole Pro or XL products that contain bundled Private Server licenses, the Get Console website sends an email to the purchasers provided email account with their order details attached. To obtain license key go to the www.get-console.com/redeem page and enter the Get Console shop order number (not invoice number) and the surname as recorded on the email into this page.

Airconsole Pro - Private Server License Redemption and Activation

Use this page to Redem your Airconsole Pro included Licences

Get Console Shop Order	<input type="text" value="4535"/>
Number:	
Surname on Order:	<input type="text" value="M"/>
<input type="button" value="Submit"/>	

If successfully matches the order number and purchasers surname in our shop then a 15 character license key will be generated and optionally emailed to the user. An example license key is "hQiv0FTE5synSno". The single license key contains all of UDIDs

Airconsole Pro - Private Server License Redemption and Activation

DO NOT LOSE THIS CODE!!

Your License Key for 2

UDID Licenses is:

Email Address for sending

code: (optional)

ACTIVATING PRIVATE SERVER LICENSE

The www.get-console.com/activation page allows for the binding of a Private Server license key to a particular Private Server.

On this page enter the license key obtained from the earlier process, and the IP address and optionally the FQDN of the Private Server that the license should be applied to. For Amazon self-hosted deployments enter the Elastic (Public) IP rather than any internal IP address.

Airconsole Pro - Private Server License Redemption and Activation

Use this page to activate your Private Server Licence Key

License Key:

Private Server IP Address:

Private Server FQDN (if used):

The IP address or FQDN + IP Address are used in the Get Console or (from v2.1) Airconsole Settings in order to share terminal sessions from these devices with Private Server. The first time the Get Console app attempts to share its terminal window with Private Server it communicates with our license server to validate that the IP Address or FQDN+IP Address match up with a licensed server so it is important that these values match and are correct.

PRIVATE SERVER WEB ADMINISTRATION

HOME PAGE

Private Server Web Manager

Home Network Files SSL Certificate Accounts Web Console **Script Manager** Settings Logout

Welcome to the Get Console Private Server

This web interface allows you to manage your Get Console Private Server. Use this management interface to change network settings, view system and uploaded from your devices logs, manage SSL certificates and User accounts. In addition this interface allows direct console access to remote iOS devices currently available as below.

Get Console Server Status **Running**

To restart/start the Get Console Private Server click [here](#)

Active Sessions:

Remote iOS Device Sessions:

Session Key	Remote Host	Device Name	Device System Model	Device System version	Connected
00755EC	111.69.33.82	AirConsole-EC	airconsole	2.10	2014-03-19 01:26:14
007F9F4	111.69.33.82	Market Place AC1	airconsole	2.10	2014-03-19 02:18:39
0450982	111.69.33.82	Simon Hope's iPhone	iPhone	7.1	2014-03-19 03:58:28
0535948	111.69.33.82	Simon's iPad Mini	iPad	7.1	2014-03-19 04:01:19

Matched Telnet Sessions:

Session Key	Remote IP Address	Connected
-------------	-------------------	-----------

Version: 1.6

Update Private Server:
To update your Private Server click [here](#)

Get Support:
Read the [User Manual](#)
See the Private Server FAQ [here](#)
Visit the Community Forum [here](#)

Our Contact Details:
Customers with a valid support contract can contact us at:
p: +6492804521
e: support@get-console.com

After connecting via web browser to the Private Server, and logging in using the default credentials (**webadmin / w3badm1n!**) the initial home screen above is displayed. With Amazon hosted Private Servers the default password is the instance ID less the dash between the first and third characters. For example if the Amazon instance ID is **i-e005c8c3** then the webadmin password would be **ie005c8c3**

The home page gives an overall view of server and the session status. The running status of the Get Console Private Server can be seen here as well as the incoming telnet and outgoing remote device telnet sessions. Should there be connecting to sessions select the restart button.

The active session from remote Airconsoles or Apple iOS devices (iPad or iPhone) are listed in the Remote iOS Device Sessions table. If these iOS device sessions have been matched to a PC or Mac user connecting to the Private Server (ie through the Private Server web site, or via a telnet client) then these are listed in the Matched Telnet Sessions table.

Note to update the Private Server software to the latest version use the link in the right side bar as identified above.

NETWORK SETTINGS

This page allows the IP address, netmask and default gateway settings to be manipulated through the web page. These are the same settings initially made via the Command Line interface.



Current Network Settings

Click on device name to change settings

Hardware: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)

Device	eth0
IP Address	121.79.197.232
Mask	255.255.255.240
Default Gateway	121.79.197.225

This page is not present in the Amazon version as this cannot be changed.

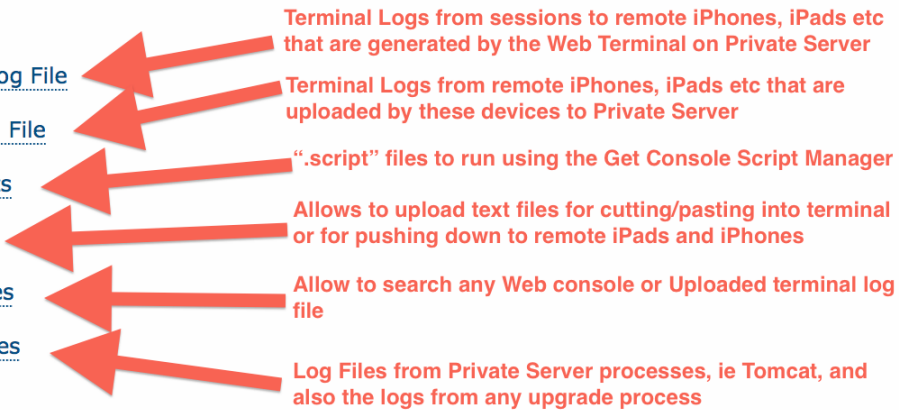
FILES SECTION

The main Files page provides access to the 3 types of Log files stored on Private Server, along with Generic text files, Configuration Scripts, and the ability to search within log files.



Files

1. [Web Console Log File](#)
2. [iOS Device Log File](#)
3. [Terminal Scripts](#)
4. [Text Files](#)
5. [Search Log Files](#)
6. [System Log Files](#)



The 3 types of log files are:

- 1) Web Console Log Files (1)– these are web-terminal session log files generated by a web user accessing an iPad/iPhone/Airconsole in the field via the Private Server’s Console web page. The logs are stored by session time and by the user that was logged into the shared session from the Private Server web console.

Files -> Remote Console Log File

Remote Console Log File		
File Name	File Owner	Action
20110826-0097571.log	webadmin	delete file

The files are owned by the Private Server user logged in and connected to the remote session. Clicking the file name link will download it.

- 2) iOS Device Log Files (2) – these are terminal session log files generated on iPads/iPhones in the field that can (if the user chooses to) be uploaded from the iOS device to the Private Server so that the Private Server has a centralized record of all in-the-field terminal activities.

Files -> iOS Device Log File

iOS Device Log File		
File Name	File Owner	Action
harbour01.txt	webadmin	delete file
log_2011-08-13_121857.txt	sergey	delete file
log_2011-08-13_125325.txt	sergey	delete file

The files are owned by the Private Server user entered on the iOS device settings at the time they were uploaded. Clicking the file name link will download it.

- 3) System Log files (6) – these are the log files used by the Private Server itself. For example the Tomcat logs, Apache logs and logs from upgrade process. These are generally for Get Console support to review during any system troubleshooting and are not that useful to end users.

In addition to these log files, the “Files” section allows for web users to upload text files (generally for cutting and pasting into terminal windows) or specialized configuration scripts that can be run by the Get Console app’s Scripting engine (Script Manager). Once uploaded and stored on Private Server, the iPad/iPhone users in the field can browse and download these text or .script files over-the-air (WIFI/3G) for use on field equipment.

Files -> Command Script Files

Command scripts:		
File Name	File Owner	Action
Priv-Exec-Prompt-Commands.txt	webadmin	delete file
3750-1-vlans.txt	sergey	delete file
ASA5510.txt	sergey	delete file

Upload Cmd Script

Click on Choose File button to choose Cmd Script file and then click Upload.

Use the Choose File and the Upload to upload config scripts/templates to the Private Server. Note that all in-the-field iOS devices will be able to see these files and download them.

ACCOUNTS

This section of the server will allow additional user accounts to be added on the server. You can add a new username and delete usernames except the webadmin user.

Accounts are used for in-the-field iPad and iPhone users to connect to the Private Server. A valid username and password must be entered in the Get Console App settings, and will be checked when connecting to the Private Server.

Private Server Management Accounts:

Username	Change Password	Delete Account
webadmin	Change Password	not available
Support	Change Password	Delete
Create New Account		

SSL CERTIFICATE

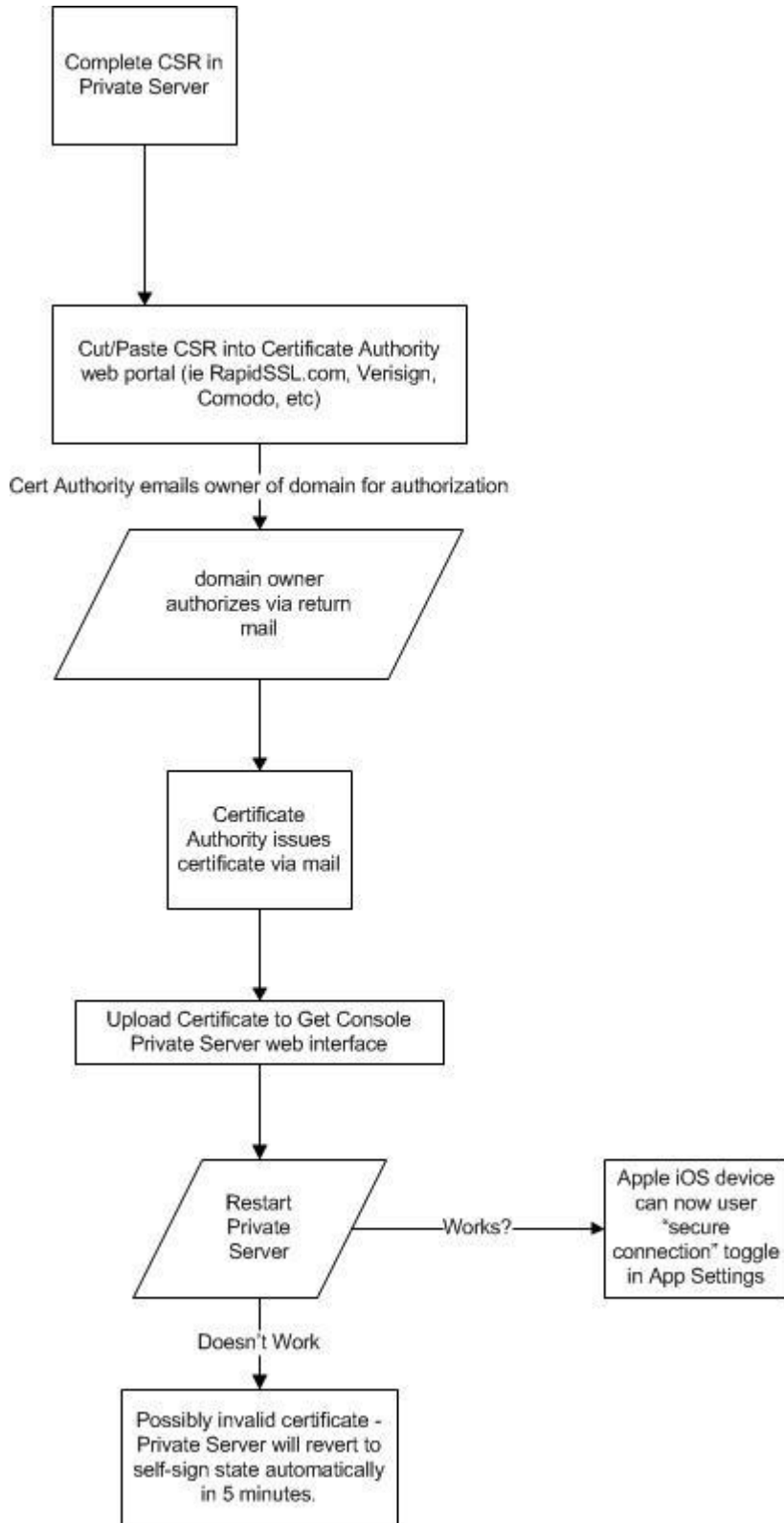
By default the sessions between the Private Server and the remote Apple iOS device are transmitted using HTTP packets. This allows faster transfer of packets from the web interface to the remote device and back (and therefore faster response to key strokes.)

By default the Private Server uses a self-signed certificate, however this will not allow “Secure Connection” to be enabled on the iOS device until a valid certificate has been issued by an issuing authority, and installed on the Private Server.

To enable SSL encryption between Apple iOS device and the Private Server a valid SSL certificate, issued by a Certificate Authority **trusted by Apple** must be installed on the Private Server. It is not possible to issue a Certificate from a private CA and use it on Private Server unless that private CA is trusted by all in-the-field iPads/iPhones. Generally it is much easier to buy and install on Private Server a low cost (\$10) SSL Certificate that is natively trusted by iPad/iPhone.

The following flowchart summarizes the process of obtaining and installing an SSL Certificate in the Private Server, and then enabling the “Secure Connection” in the iOS device App Settings. After the flow chart a detailed example of obtaining and installing an SSL certificate is covered.

Note that wildcard certificates are not supported to be imported by the web gui. If you have a wildcard certificate that needs to be installed contact us at support@get-console.com for CLI instructions.



GENERATE CERTIFICATE SIGNING REQUEST

To enable SSL encryption in the Get Console Private Server the first step is to Generate a CSR (Certificate signing request)

The screenshot shows the 'Private Server Web Manager' interface. At the top, there is a navigation bar with links for Home, Network, Logs, SSL Certificate, Accounts, Console, and Logout. The 'SSL Certificate' section is active, displaying instructions on how to secure the connection between an Apple iOS device and the Private Server. It includes a list of steps: 1. Generate CSR (Certificate Signing Request), 2. Upload Certificate Files, and 3. Restart Private Server to apply the new SSL Certificate. The current certificate is identified as '(User Certificate: /getconsole/ssl/cert/ps1.cloudstore.co.nz_Sergey.crt)'. A sidebar on the right provides support information, including links to the User Manual, Private Server FAQ, and contact details for customers with a valid support contract.

The following form will be presented – complete this form using your own company and Common Name information :

SSL Certificate -> Generate CSR

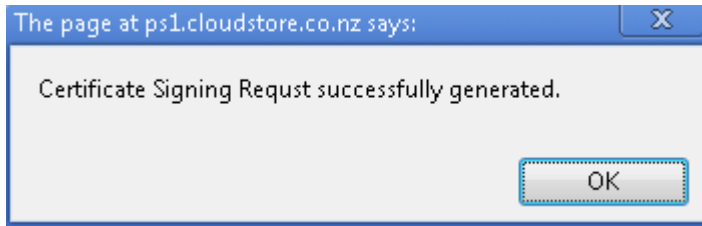
Please fill the form below to generate the Certificate Signing Request (CSR):

The form is titled 'Country Name:' and contains several input fields. The 'Country Name' is a dropdown menu set to 'United States of America'. The 'State or Province Name (eg, Florida):' field contains 'Auckland'. The 'Locality Name (eg, Miami):' field also contains 'Auckland'. The 'Organization Name (eg, Miami Field Services Inc):' field contains 'Cloudstore'. The 'Organizational Unit Name (eg, Engineering):' field contains 'Test'. The 'Common Name (eg, the Fully Qualified Domain Name you have given to this Private Server for example: getconsole.miamifieldservices.com):' field contains 'ps1.cloudstore.co.nz'. The 'Email Address:' field contains 'simon@cloudstore.co.nz'. At the bottom of the form is an orange button labeled 'Generate CSR'.

Fill in the details of you country location, organization, name and email address. The Common Name of your organization must be a fully qualified domain name (FQDN) that you will allocate to the Private Server. This

is the most important part of the form as the certificate authority will run a query to find out who the owner is of the domain and email them to authorise the certificate request. Also the FQDN defined must be resolvable in DNS by the iOS devices.

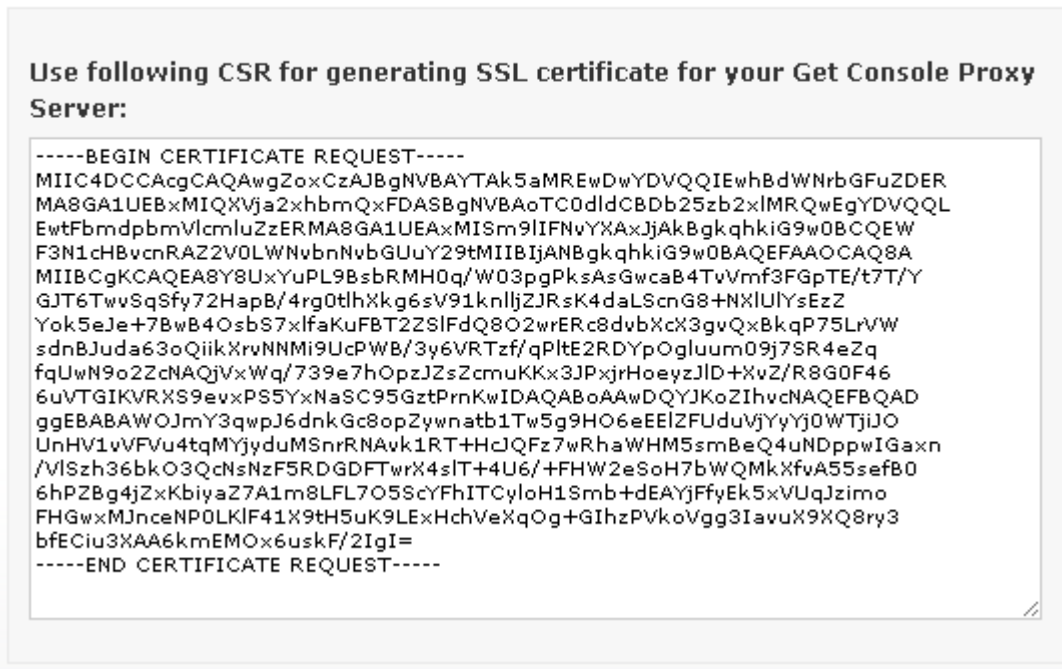
Once this form has been filled in correctly a message will be displayed that the Certificate Signing Request has been successfully generated. Click OK



In the window that opens up the CSR will be listed. Copy and store this text to clipboard.

Include the -----BEGIN CERTIFICATE REQUEST----- , -----END CERTIFICATE REQUEST----- lines in the your clipboard copy

CSR:



OBTAINING SSL CERTIFICATE

Next you will need to contact a Certificate Authority. Different Certificate Authorities have different processes for submitting CSRs, and in turn issuing the SSL Certificate. However generally the process follows as below:

Once you have paid for the certificate and submitted the CSR, the Certificate Authority organization will perform a WHOIS on the domain owner, and then email the FQDN (common name) owner for authorization to issue a certificate. Once the domain owner has mailed an approval back to the Certificate Authority (usually by clicking a link in an authorisation request email) they will send through a certificate in .crt

format. If the Certificate Authority offers an option as to the format of the Certificate then choose **Apache .crt format** Upload this certificate using the process as below:

UPLOAD SSL CERTIFICATE TO PRIVATE SERVER

Using the “upload certificate file” link on the SSL Certificate page will take you to a page where you can select and upload the certificate you have been issued and upload it to the Private Server:

SSL Certificate -> Upload Certificate

Current SSL Settings

Virtual Appliance SSL Settings:

[SSL Certificate File](#) /getconsole/ssl/cert/ps1.cloudstore.co.nz_Sergey.crt

Click on SSL setting name in the table above to change it

SSLCertificateFile

Click on Choose File button to choose new SSL Certificate File and then click Upload.

Choose File

Upload

Once you have done this you will need to reload the server on the original SSL Certificate page. If the certificate is invalid the server will automatically revert to a self-signed certificate status within 5 minutes.

SSL Certificate

To make the connection between the Apple iOS device and the Private Server more secure, upload a SSL certificate to your private server here and then enable the "Secure Connection" option in the Get Console app.

1. [Generate CSR \(Certificate Signing Request\)](#)
2. [Upload Certificate Files](#)
3. [Restart Private Server to apply the new SSL Certificate](#)

Current certificate: **(User Certificate:**
/getconsole/ssl/cert/ps1.cloudstore.co.nz_Sergey.crt)

Valid SSL Certificate Running. The "Secure Connection" option on the Apple iOS Get Console app CAN be used

Once the SSL Certificate has been successfully installed, the SSL Page will show the green “User Certificate” as above.

Note as above that wildcard certificates are not supported to be imported by the web gui. If you have an existing wildcard certificate that needs to be installed contact us at support@get-console.com for CLI instructions.

The in-the-field Apple iOS devices and Airconsole will now be able to use the “Secure Connection / SSL” setting. If this setting is selected while a self signed certificate is still installed on the Private Server an error about invalid Private server will appear.



UPDATING THE PRIVATE SERVER SOFTWARE

Starting from Private Server version 1.5.1, the Virtual Appliance and Database files can be updated without re-installing the Virtual Appliance. This feature will be used to non-disruptively update Private Servers from version 1.6 to version 1.7 and later.

There are 2 methods to update the Private Server software

- 1) Semi-Automatic Updates
- 2) Manual Updates

Although the Get Console developers test all Private Server updates, There is currently NO option to rollback an update after it has been installed. Because of this we recommend using the VMWare or “Snapshot” facility to take a Snapshot of the Virtual Appliance before applying the update. Should an update cause corruption to the Private Server, revert to that VMWare snapshot and contact Get-Console support.

SOFTWARE UPDATES

There are 3 options on the Software upgrade page.

Update Options:

1. [Update your Private Server automatically \(Internet connection required\)](#)
2. [Update your Private Server manually](#)
3. [Update web server to the latest version \(Internet connection required\)](#)

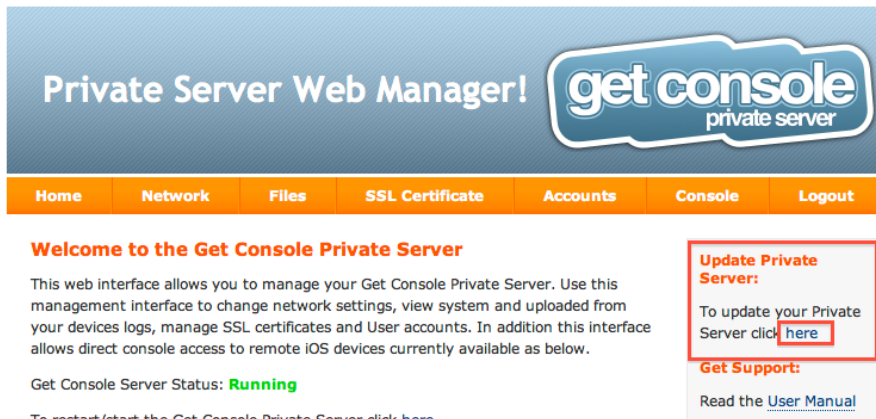
- 1) Upgrades between a point release can generally be performed automatically for example an upgrade from version 1.5.1 to version 1.5.2
- 2) Upgrades between major releases (1.5.1->2.0.0) and **some** minor releases (1.5.1 -> 1.6.0) can only be performed via the manual method. This will be noted on the www.get-console.com/private-server page.

- 3) Upgrades to the underlying Apache server can be performed automatically and independently of the Private Server. We recommend checking and patching the webserver regularly to keep web security vulnerabilities minimized.

AUTOMATIC UPGRADES

The Semi-Automatic update process involves checking the Get-Console.com website for new Private Server sub versions for the Major.minor release currently installed, if a new version exists downloading it and then if downloaded successfully, installing it. No restart of the Private Server is generally required.

To check for new versions of Private Server click the “Check for Updates” button on the home page (or any of the other Private Server pages) located on right hand side bar



Select option 1: Automatic Updates (Requires Internet Connectivity)



If a new update is available then it will be presented as available to download – in the case below version 1.2.0 can be upgraded to 1.2.1 is available:



After downloading, the dialog box will allow for installing

Download Private Server update to version 1.2.1:

The screenshot shows a web interface with two main sections. The top section is titled "Download Update 1.2.1:" and contains a single orange "Submit" button. Below this, a message states "Update file was downloaded successfully." The bottom section is titled "Install Private Server version 1.2.1:" and contains a label "Install update:" followed by an orange "Submit" button. A red rectangular box highlights the "Submit" button in the "Install update:" section.

Clicking on "Submit" button under Install Update will install the downloaded patch file. The patch file will unpack and install the changes to the Virtual Appliance. The last line should say "DB successfully updated".

Install Private Server version 1.2.1:

The screenshot shows the "Install update:" section with an orange "Submit" button. Below this, a red-bordered box contains the "Update Log:" which lists the following files and actions:

- Archive: /var/www/update/gcprsupdate1.2.1.zip
- inflating: /var/www/functions_mgmt.php
- inflating: /var/www/update_db.php
- inflating: /var/www/html/css/style.css
- extracting: /var/www/html/img/button.png
- inflating: /var/www/html/img/files/button1.jpg
- inflating: /var/www/html/img/files/button1_active.jpg
- extracting: /var/www/html/img/files/form_button.png
- extracting: /var/www/html/img/files/form_button_over.png
- extracting: /var/www/html/img/files/icons.png
- inflating: /var/www/html/img/files/Thumbs.db
- inflating: /var/www/html/img/files/transparent.gif
- inflating: /var/www/html/img/files/upload-button-active.jpg
- inflating: /var/www/html/img/files/upload-button.jpg
- extracting: /var/www/html/img/login-background.png
- inflating: /var/www/html/index.php
- DB was successfully updated.

MANUAL UPDATES

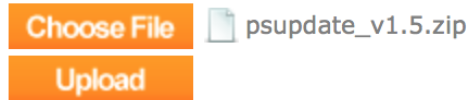
The Manual Update process requires the download of the update package from the get-console.com/private-server webpage, and then uploading this package to the Private Server.

Generally the Manual Update method will be needed when many O/S level files need to be patched or added. This means that the server will be rebooted during the upgrade process.

Update Options -> Update your Private Server manually

To manually update your Private Server visit our website - <http://www.get-console.com> and upload an update file using the form below.

1. Click on Choose File button to choose Update File and then click Upload.

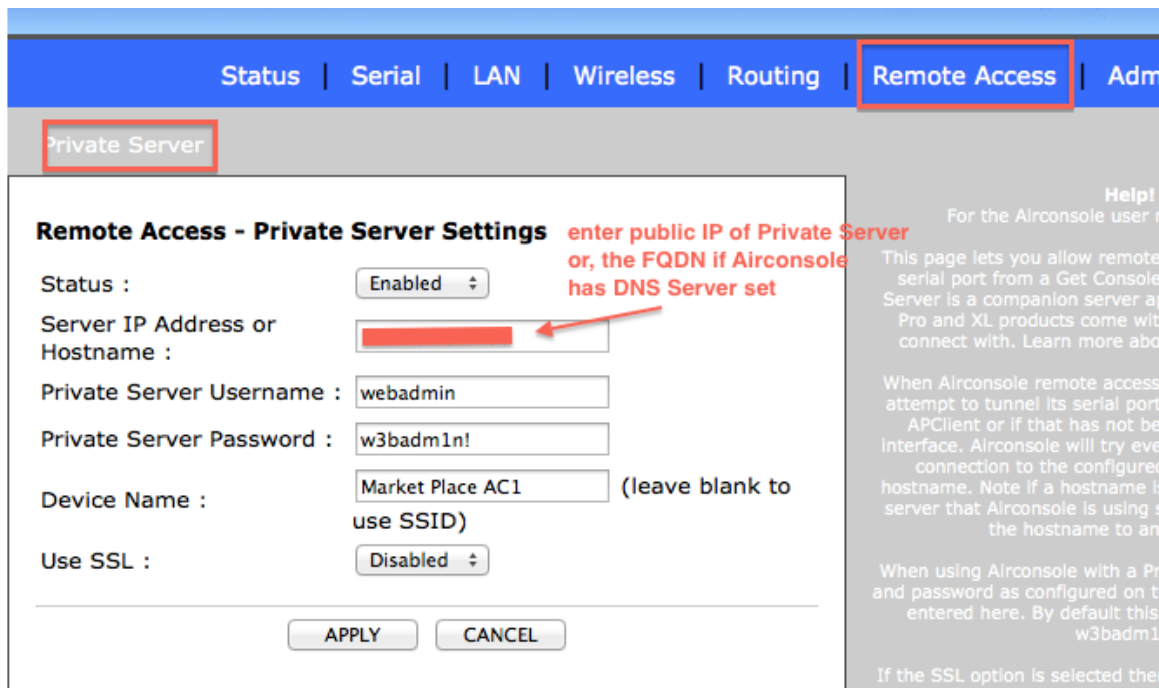


After uploading, click Submit button under the "Install update" heading. Note the checkbox to perform the install unattended. Clicking submit button will reboot the server, and during the reboot the server will unpack the update zip file and run the associated install scripts. This process can be viewed via the VMWare console if

If the unattended install check box is NOT ticked, then the update script will prompt user for confirmation of the script to run and timing of the reboot via the VMWare console terminal. The terminal needs to be accessed within 30 seconds of pressing submit or the upgrade will be cancelled and the original version of the Private Server will boot.

CONFIGURING AIRCONSOLE ADAPTOR TO USE PRIVATE SERVER

To enable a particular Airconsole device to use the Private Server, 3 fields must be populated correctly in the Remote Access -> Private Server Settings:



- 1) the IP address or FQDN details of the Get Console Private Server. An FQDN is needed to support the SSL option. These details **MUST** match the details in the license activation process described in above licensing section.
- 2) a valid username for a user defined on the Private Server must be entered into username field (for example "webadmin" is the default user)

- 3) the password for that Private Server hosted username must be entered correctly (for example **"w3badm1n!"** for self hosted, or the Amazon instance ID (minus the "-" character) for Amazon Hosted Private Servers.

Set the Status to be **Enabled**, and optionally enable SSL if your Private Server has an installed SSL Certificate.

When the status is enabled, the Airconsole will attempt to connect to the Private Server. It will try every 10s, 20s, 30s, 40s and then once every minute until it is successful. To be successful it must have IP connectivity to Private Server. Generally this is achieved by either the AP Client feature or by connecting the wired Ethernet port of the Airconsole into an existing network and configuring Airconsole as a DHCP Client. These configuration options are contained in the Airconsole User manual available at www.get-console.com/airconsole

When Airconsole is connected to Private Server successfully it will show the status in the Airconsole homepage

Airconsole Details

Firmware Version :	2.10 (2014-03-18 build 441)
Hardware Version :	A-01
Host Name :	AirConsole-F4
Operating Mode :	AP Client
Bridge IP :	192.168.10.1
AP Client IP :	10.64.8.93
DNS Servers :	202.37.101.1, 203.97.78.44, 8.8.8.8
Remote Access :	Connected to 121.79.197.233, key=007F9F4

Copyright © 2014 Cloudstore Limited
For support please contact us at: support@get-console.com

CONFIGURING IOS DEVICE GET CONSOLE APP TO USE PRIVATE SERVER

To enable a particular Apple iOS device to use the private server, 4 fields must be populated correctly in the Get Console app Settings:

- 1) the IP address or FQDN details of the Get Console Private Server. An FQDN is needed to support the Secure Connection option. These details **MUST** match the details in the license activation process described in above section.
- 2) a valid username for a user defined on the Private Server must be entered into username field (for example **"webadmin"**)
- 3) the password for that Private Server hosted username must be entered correctly (for example **"w3badm1n!"** for self hosted, or the Amazon instance ID (minus the "-" character) for Amazon Hosted Private Servers.
- 4) the Remote Server setting must have "Private Server" selected (as opposed to North America, Asia Pac or Europe)

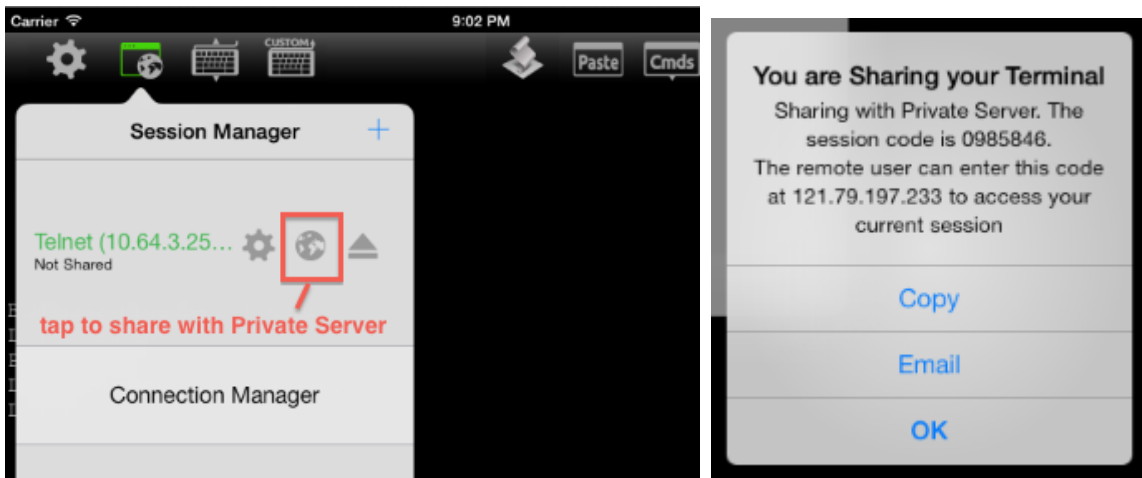
Please note that ALL fields are **case sensitive**

Do NOT enable the “Secure Connection” switch in the App until a valid SSL Certificate has been installed on the Private Server. See the SSL Certificate Section below.

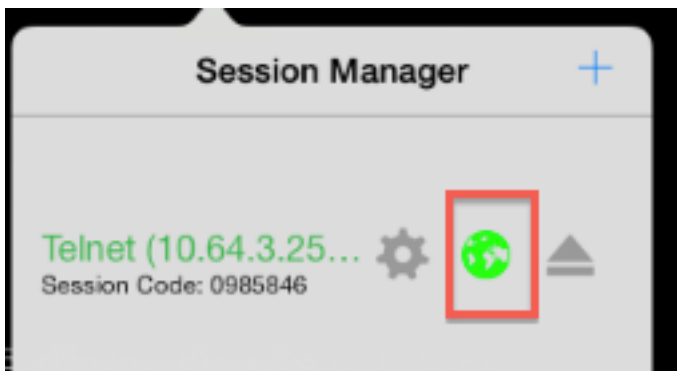
An example of valid iOS device settings is below:



Once these settings have been configured, return to the main terminal window in the App, and press the Connect Session button (top nav bar in Terminal window, second from left button), and then select “Share Session”

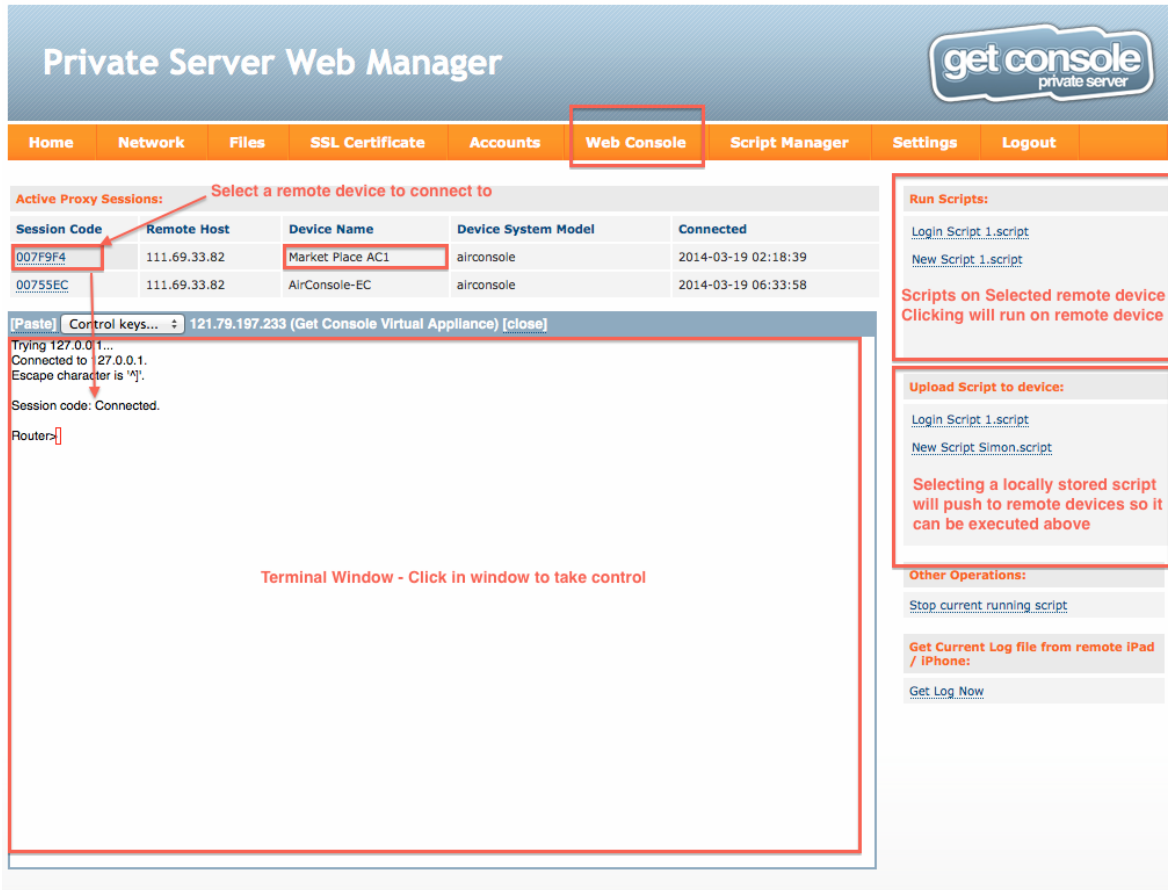


Once the session is shared, a pop-up appears in the iOS device provides the allocated session code. Session codes to Private Servers always start with “0” The Globe icon will be green when session is being shared:



ACCESSING REMOTE TERMINALS

Once the remote iPad/iPhone or Airconsole is connected to Private server, its session will show up on the Private Server home page. Clicking on the Web Console link on the home page will navigate to the Private Servers web terminal interface where the remote device can be selected and accessed.



Selecting a session code from the available list will connect the web terminal to the remote Airconsole/iOS Device. After connecting, the Private server will also query the remote Airconsole/iOS installed scripts and populate the "Run Scripts" box on the right hand side.

Clicking in the terminal window will provide direct CLI access to the remote device connected through the Airconsole/iPhone/iPad serial port.

Clicking on a script from the Run Scripts box will invoke the execution of that script via the remote Airconsole/iPhone/iPad.

If the remote Airconsole/iPhone/iPad does not have a needed script it can be pushed down to it via clicking any of the local Private Server scripts listed in the "Upload Script to Device" box. To create or edit local Private Server scripts go to the Script Manager page (discussed below).

The PC/Mac web user can also use a generic telnet client to access to remote iOS device serial terminal session using port 2323. To use a third party telnet client rather than the web client, simply telnet to the Private Servers IP address (or domain name) on TCP port 2323. A session code prompt will be presented where the PC user can enter the code of the remote iOS or Airconsole device to be connected.

SCRIPT MANAGER

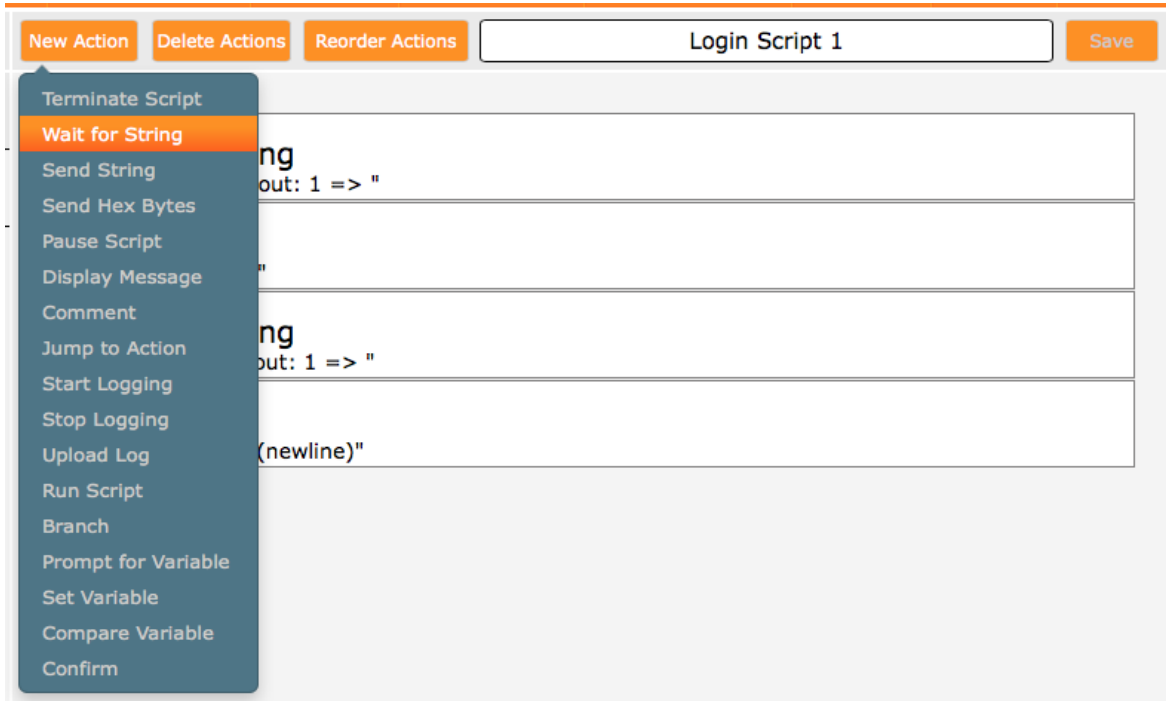
Private Server version 1.6 includes a web version of the Get Console Script Manager built in. This is an easy GUI based web tool for creating, modifying and deleting terminal scripts for use in both Get Console iOS App, and also for remote execution on Airconsole devices.

Private Server Script manager can read in any existing script created in Get Console app, and also allows for the scripts to be saved out to the users desktop. The files are xml “.script” files that are compatible with all our products.

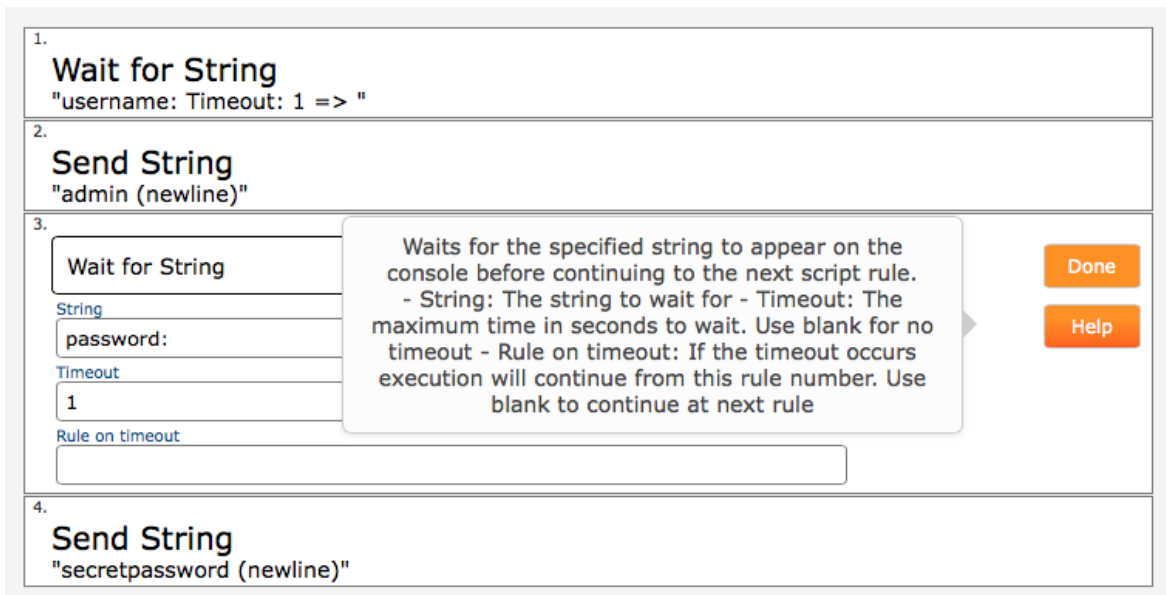


As the above screen shot shows, complete creation and editing of terminal scripts can be achieved on this single page. The left box identifies all of the available scripts currently saved on the Private Server. The highlighted script will be opened in the right pane for editing. New actions can be added to the bottom of the script via the New Action dropdown list.

Script actions can be re-ordered via the Reorder Actions button that enables drag and drop to move action items around.



Clicking any individual action allows it to be edited, while mousing over the Help will bring up help for the fields needed for this particular action. Click Done when finished making any changes to the Action item.



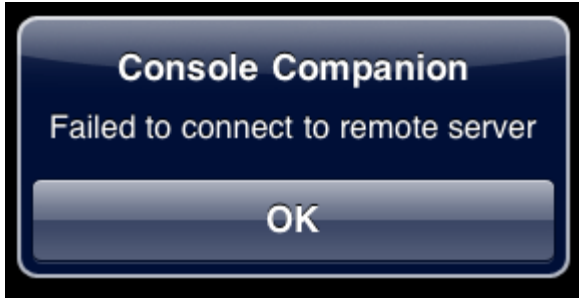
Most scripts are used to automate login or to collect information from a device for use in other processing. The above example is a simple login script.

Action 1 Wait for String will wait for the terminal window to present a "username:" prompt, and if seen it moves to the Action 2 – Send String where "admin" is sent back to the terminal with a carriage return ("newline"). The script then has another Wait for String action looking for "password:" prompt to appear, and if it does then Action 4 responds with "secretpassword" and carriage return.

For more detail on all the possible Script actions, please refer to the Get Console user guide available at www.get-console.com/faq

TROUBLESHOOTING CONNECTIVITY TO PRIVATE SERVER

GENERAL CONNECTIVITY ISSUES

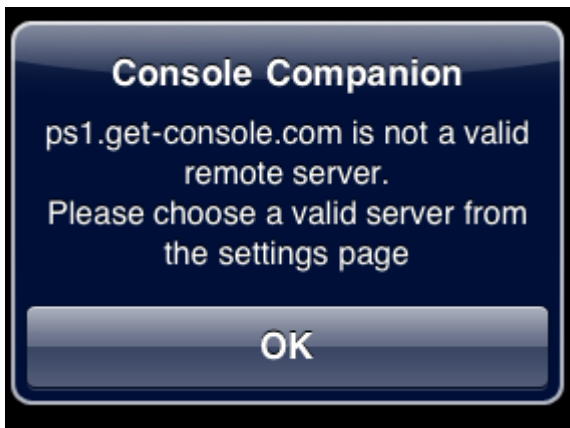


The above message will be displayed on the apple iOS device when:

- 1) There is no connection to the internet or private network where the Private Server resides; or
- 2) The FQDN of the Private Server (if configured as FQDN rather than IP address) cannot resolve to an IP address via the iOS device; or
- 3) The Private Server is nor reachable (switched off, not routable or possibly firewalled on ports 80 or 443)
- 4) **Where "Secure Connection" is selected in the Get Console App, but no valid SSL Certificate has been installed on the Private Server**

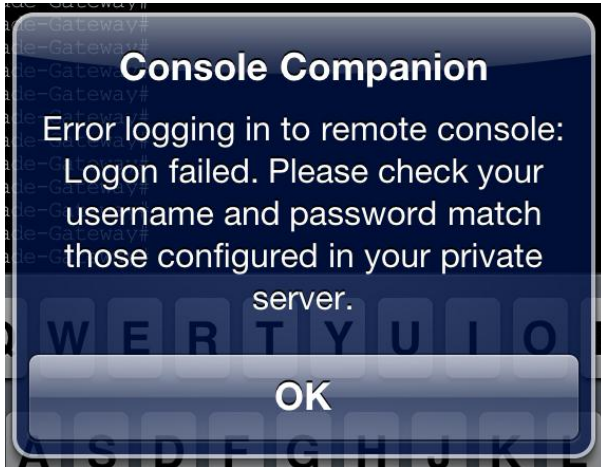
Please correct the connectivity issues for the iOS device or Private server, or disable "Secure Connection" in settings then try again.

SERVER NOT RECOGNIZED BY LICENSE SERVER



The above message will be displayed on the Apple iOS device when although there is internet connectivity for the iOS device, the Private Server IP address or Hostname has not yet been enabled on our license server. Please purchase a license from the www.get-console.com/shop or if one has been purchased already please provide the server details to activations@get-console.com to ensure it has been activated.

INCORRECT USERNAME OR PASSWORD



This error occurs when username has either not been defined on Private Server (Accounts tab), or has been defined but the password is wrong. Note that both Username and Password are case sensitive.

LICENSE ISSUES

Where the Private Server is defined on our License Server, but does not have any available licenses then when connecting the user will receive an error like below.



The possible error codes (useful for Get Console Support) are:

0001 = Private Server Defined but no License Assigned

0002 = Private Server Defined, License Assigned but no un-expired licenses available

0003 = Private Server Defined, License Assigned but all existing licenses are used up by other devices

Other error codes maybe added in the future. In all these cases if you have purchased a Private Server license from the Get Console shop and requested its activation/assignment but are still receiving this error then please contact Get Console support via email at support@get-console.com

When using the www.get-console.com/activation method to load licenses onto Private Servers, the process takes around 2 minutes. For manually activated licenses there is a lead time of 4 hours from purchase for our staff to upload the CAL license details to the license server.

