



User Manual

Get Console Private Server

Version: 1.20

Date: 5 September 2011

CONTENTS

Revision History	3
What Is Get Console Private Server?.....	3
Get Console App	3
Get Console Server.....	4
Obtaining the Private Server Software.....	6
Virtual Appliance Requirements	6
Firewall Port Requirements	6
Common Deployment Architecture	8
Installing VMWare Appliance	9
Installing with VMWare Server	9
Installing with VMWare vSphere	10
Initial Network Configuration	12
Private Server Licensing.....	12
How licensing works	12
Licence activation procedure	13
Private Server Web Administration	14
Home Page	14
Network Settings.....	14
Files Section	15
Accounts.....	16
SSL Certificate.....	17
Generate Certificate Signing Request	18
Obtaining SSL Certificate.....	20
Upload SSL Certificate to Private Server	21
Updating the Private Server Software.....	22
Automatic Updates	22
Manual Updates.....	24
Configuring iOS Device Get Console App to use Private Server....	24
Troubleshooting Connectivity to Private Server	28

General Connectivity Issues	28
Server Not Recognized by License Server	28
Incorrect Username or Password.....	28
License Issues.....	29

REVISION HISTORY

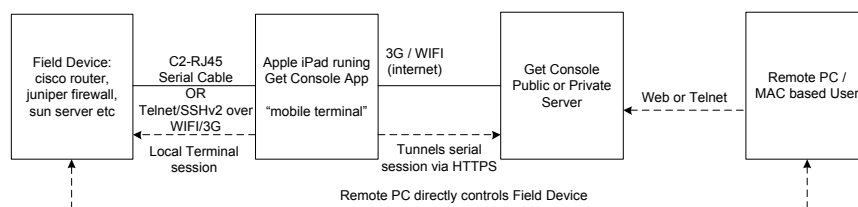
Revision	Date	Description	Author
1.04	5 May 2011	First Release	SH / RP
1.20	30 August 2011	Second Release for Private Server v1.2	SH / RP

WHAT IS GET CONSOLE PRIVATE SERVER?

There are 2 Components to the Get Console solution

- 1) 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(v2)** 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.

GET CONSOLE SERVER

There are 2 versions of the Get Console Server

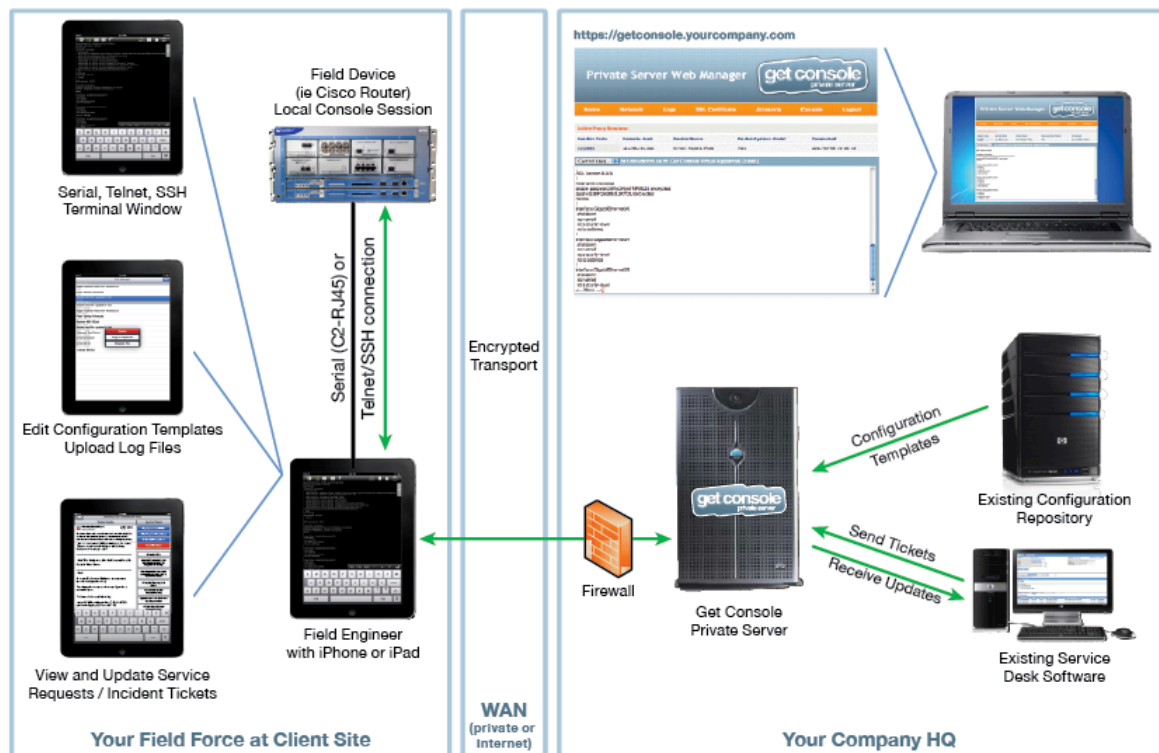
- 1) The publicly available Get Console Servers hosted at the website www.get-console.com
- 2) The private version, which is hosted on a customers own network, and secured by their own network security policy (the subject of this user manual).

Both versions of the Get Console Server acts as a connection broker and proxy between the Apple iPad/iPhone terminal session and the remote users sitting at PCs, allowing the remote PC user to control the terminal session connected to the Apple iPad/iPhone.

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 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:

- Increased Security, as the Private Server and Remote PC user are 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.
- Increased Performance, as the latency between the Remote PC user and the Private Server is greatly reduced meaning the end to end performance of the remote control terminal session is fast and smooth
- Increased Flexibility, as the Remote PC user can use either the Private Servers built in Web Terminal, or any Telnet client of their choosing (such as SecureCRT, or puTTY)
- Increased Ease of 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.
- Upload and Manage corporate configuration templates for field devices and download them to the iPad/iPhone in the field
- 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 a free download available from the www.get-console.com/download website. The 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 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.

VIRTUAL APPLIANCE REQUIREMENTS

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

The next version of Private Server (v1.3) will participate with an existing corporate trouble ticket system, 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). Consider provisioning this account to be ready for the v1.3 update patch.

FIREWALL PORT REQUIREMENTS

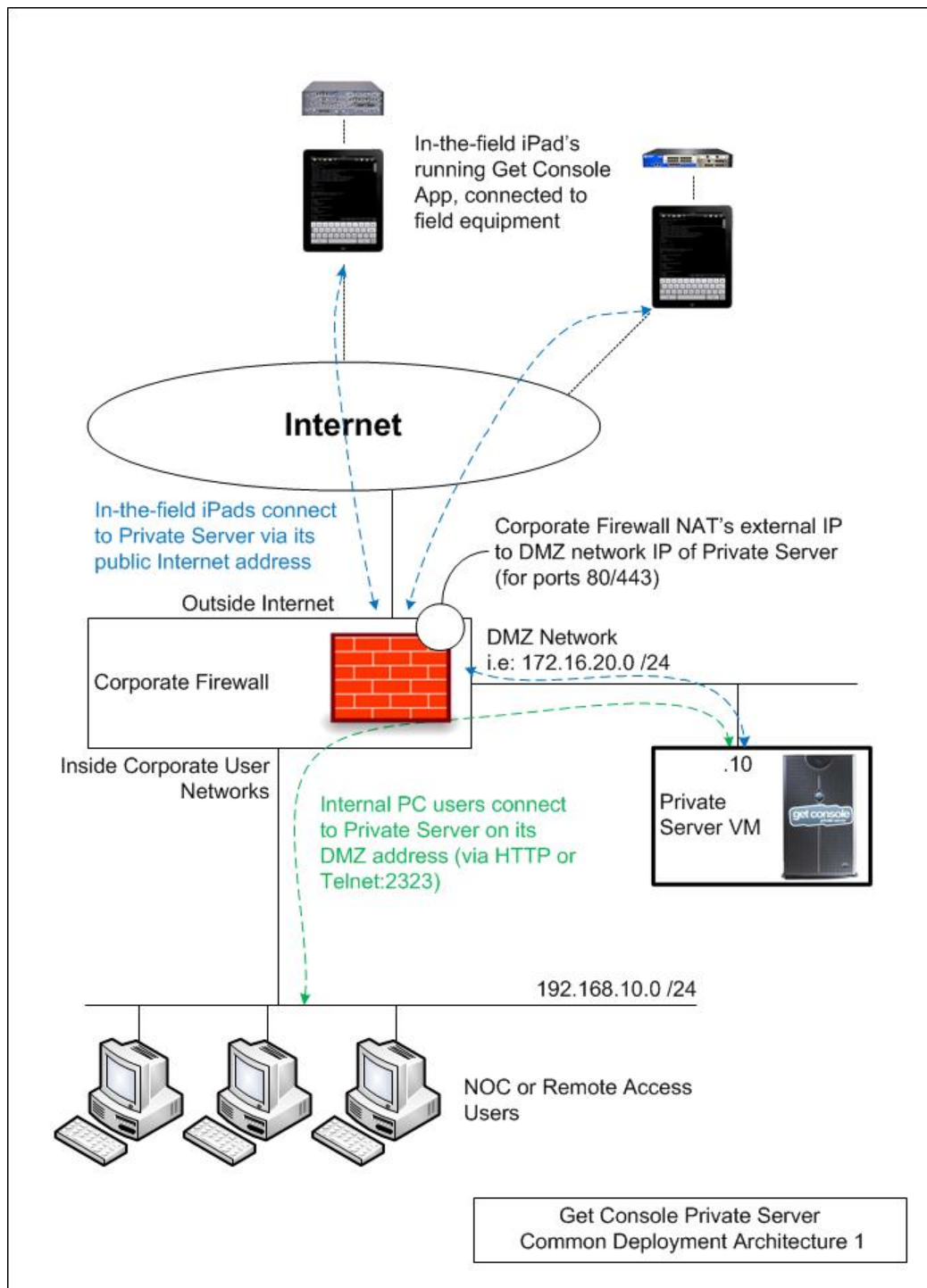
The following Table describes the ports used by the Private Server. These ports will need to be open to the Private Server from any intervening firewall.

TCP Port	Description	Used For
80	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	HTTPS	(Where SSL certificate has been installed, and

		<p>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</p> <p>This port is also used outbound from the Private Server to check the www.get-console.com website for software updates.</p>
2323	Telnet	From NOC/Remote User PC to Private Server (if using third party telnet client (ie SecureCRT/Putty)
25	SMTP	(optional – for later use in v1.3) 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	POP	(optional – for later use in v1.3) used from Private Server to download its troubletickets from its user provided mailbox on the Corporate email system

COMMON DEPLOYMENT ARCHITECTURE

The below drawing describes the most common high level network design for deploying 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 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.

INSTALLING VMWARE APPLIANCE

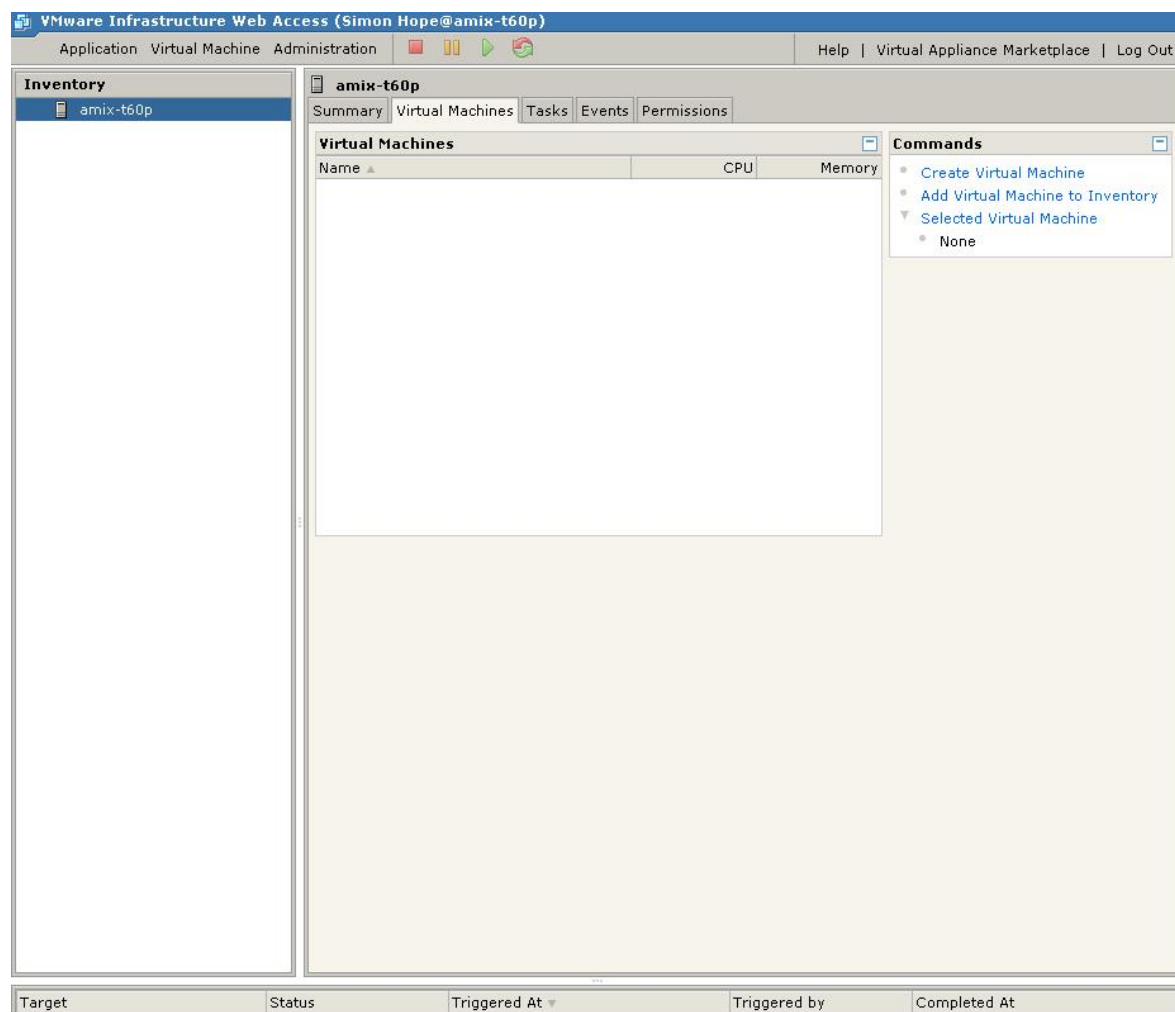
This section provides instructions for installing the Get Console Private Server on either VMWare Server 2.0 (free) (Vmx/VMDK package), or on a VMWare vSphere Cluster (OVF package). Other VMWare platforms should follow the VMWare Server instructions. Non VMWare platforms should work however are not officially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



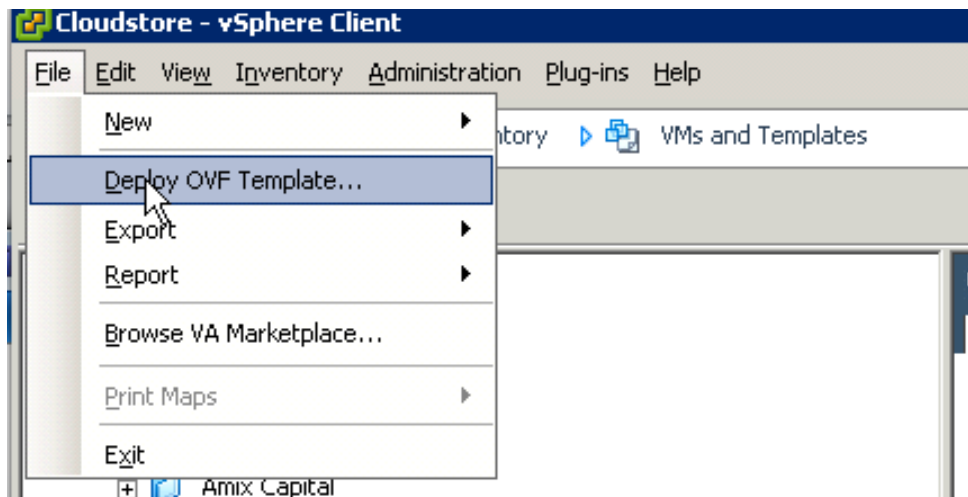
Select the .vmx file from the unzipped package from the get console web site and click open. The appliance will install.

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

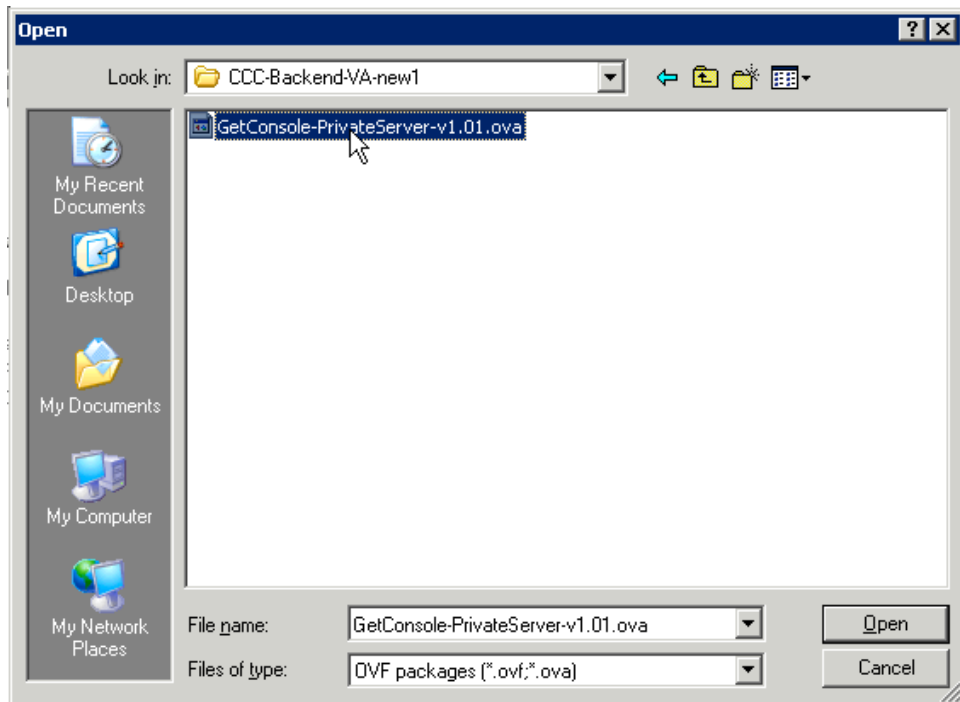
Select the play button to start the appliance. Follow the Initial Network Configuration Instructions and Web administration sections below to complete the installation.

INSTALLING WITH VMWARE VSPHERE

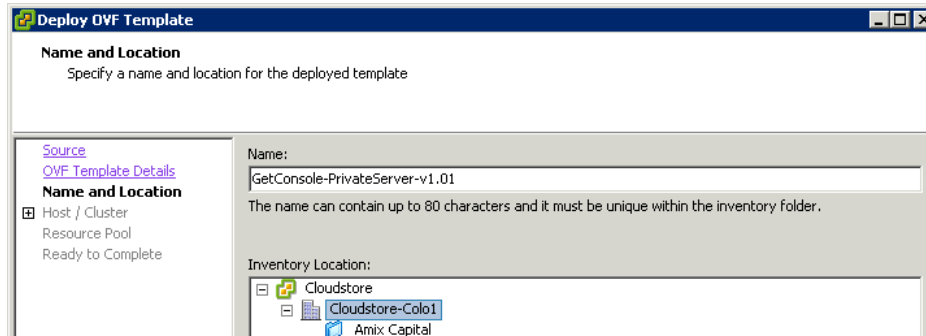
To setup the Private Server with vSphere, download the image to a datastore repository visible to the vSphere server(s). Either the VMX/VMDK or OVF package will work with vSphere. The instructions below use the OVF package.



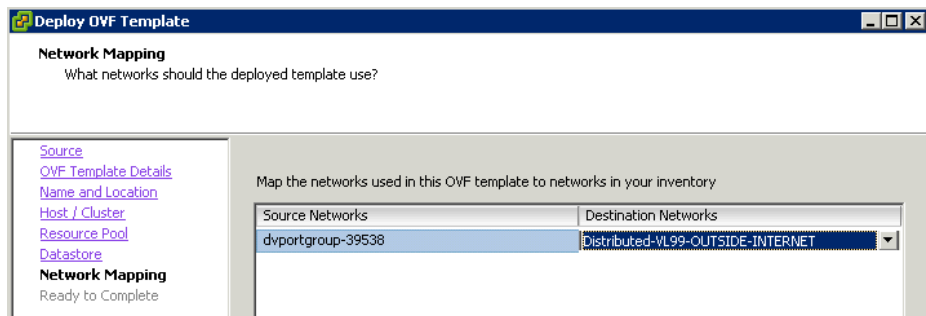
Select the .OVA file from the downloaded package (for method to install .vmx use the New Virtual Machine wizard using the vmx/vmdk as the existing VM disk)



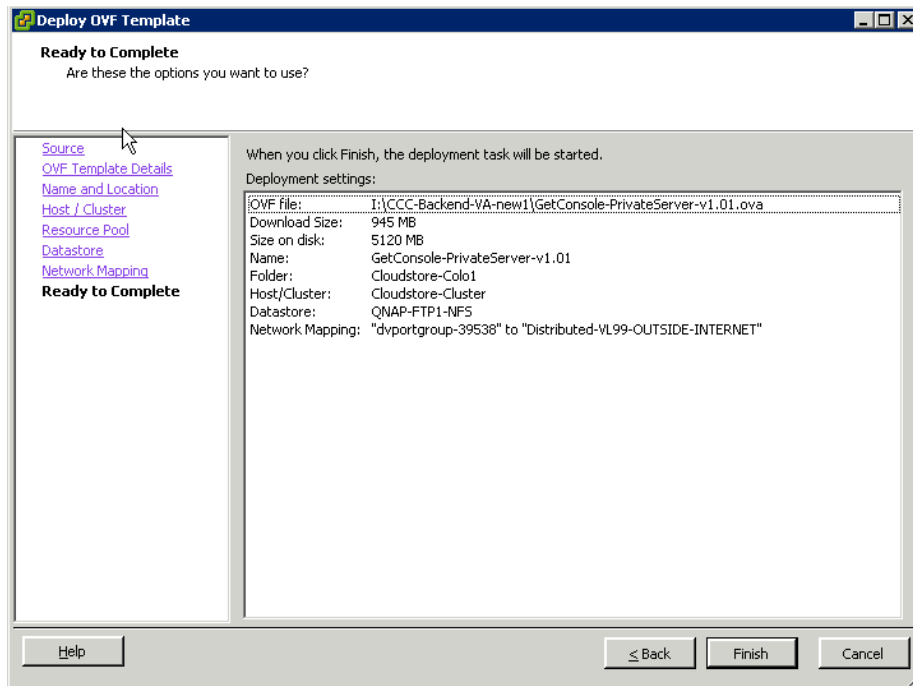
Follow "Deploy OVF Template" Wizard



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:

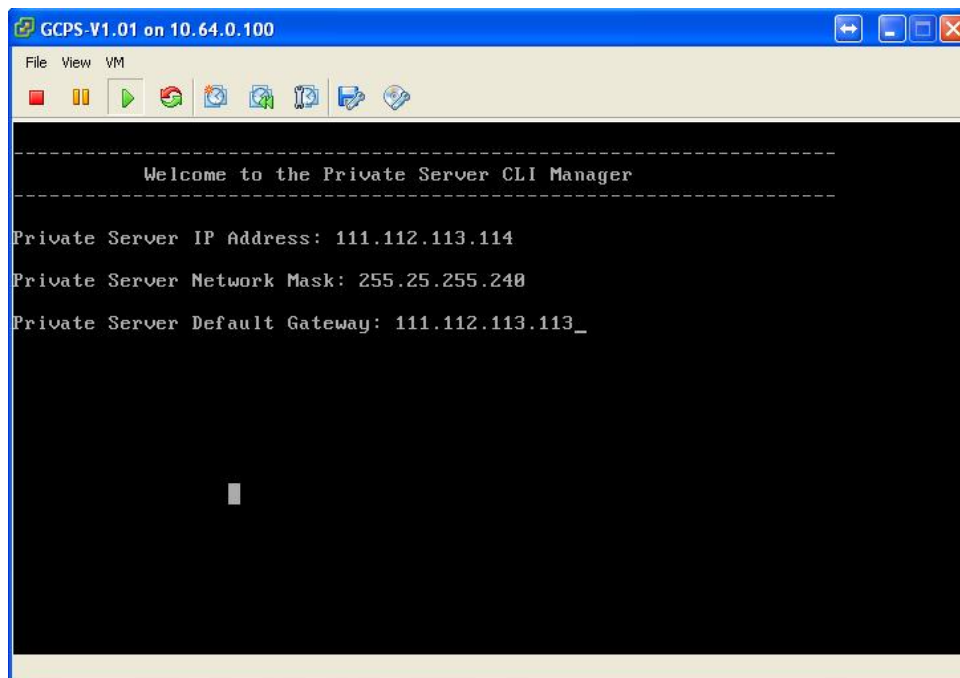
Once the Private Server is available in VMWare and has been booted, launch the Virtual machine Web Console. A Centos console will be presented with a login and password prompt.

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 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.

The CAL is enforced when the Apple iOS device tries to connect to the Private Server for the first time. On first connection, the Apple iOS device will initially make a check with our license server to see if the Private Server as configured in the Apple iOS device has free licenses available, and if so will store the iOS device UDID 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 will receive instructions on how to allocate these licenses against their private server. At the time of writing, the process requires the purchaser to advise Get Console via email (activations@get-console.com) of the server IP/FQDN of their Private Server, and the invoice number of their purchase. Within 4 hours these licenses will be added to the Get Console license server as belonging to the purchasers Private Server's IP address. An email will be sent confirming license activation.

PRIVATE SERVER WEB ADMINISTRATION

HOME PAGE

Private Server Web Manager



[Home](#) | [Network](#) | [Files](#) | [SSL Certificate](#) | [Accounts](#) | [Console](#) | [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** Green is good!

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

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

Version: 1.2

Active Sessions:

Summary of active connections running through Private Server at the moment

Remote iOS Device Sessions:

Session Key	Remote Host	Device Name	Device System Model	Connected
0053427	203.97.151.146	Simon's iPad	iPad	2011-08-26 15:18:16

Matched Telnet Sessions:

Session Key	Remote IP Address	Connected
0053427	127.0.0.1	2011-08-26 15:18:04

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

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 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 that sessions matched to a user that is connecting via the Private Servers web based terminal will be displayed as 127.0.0.1.

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.



Private Server Web Manager

Home Network Logs SSL Certificate Accounts

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

FILES SECTION

The main Files page provides access to the 3 types of Log files stored on Private Server, along with Configuration Scripts that can be stored on the server for downloading to iPads and iPhones in the field.



Private Server Web Manager

Home Network **Files** SSL Certificate Accounts Console Logout

Files

- [System Log Files](#) → logs generated by the Private Server itself - ie Apache / Tomcat
- [Remote Console Log File](#) → Log files from Web terminal (console) connections to remote iPads / iPhones
- [iOS Device Log File](#) → Log files uploaded from iPads / iPhones in the field
- [Command Script Files](#) → Configuration Scripts / Templates that can be downloaded to iPads / iPhones in the field

Get Support:

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

Our Contact Details:

Customers with a valid

The 3 types of log files are:

- 1) System Log files – these are the log files used by the Private Server itself. These are for Get Console support to review during any system troubleshooting and are not that useful to end users.
- 2) Remote Console Log Files – these are web-terminal session log files generated by a web user accessing an iPad/iPhone 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.

- 3) iOS Device Log Files – these are terminal session log files generated on iPads/iPhones in the field that can 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.

In addition to these log files, the “Files” section allows for web users to upload configuration scripts (text files) to the Private Server. Once uploaded and stored on Private Server, the iPad/iPhone users in the field can browse and download these 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.

Choose File

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		

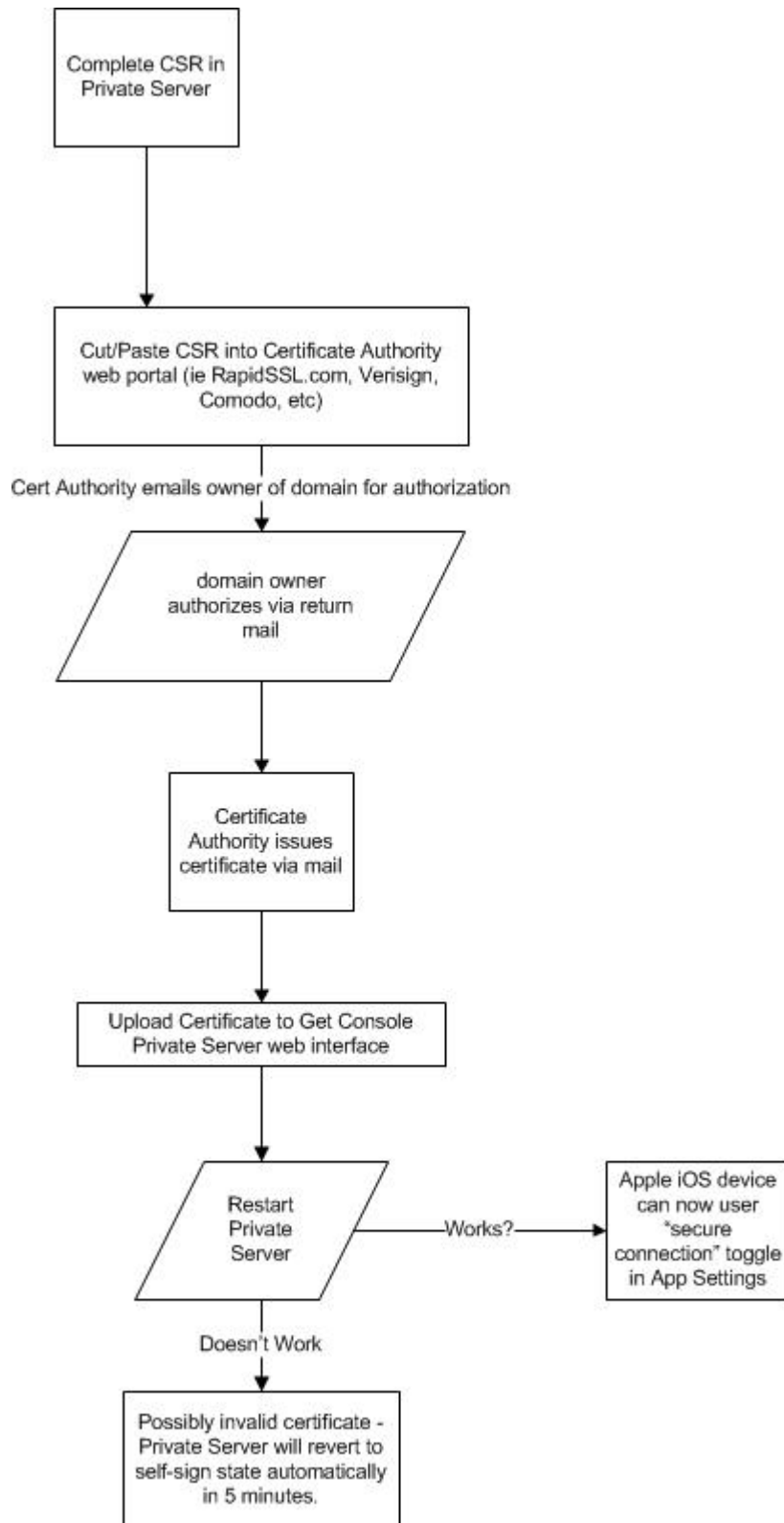
SSL CERTIFICATE

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.



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)

Private Server Web Manager



[Home](#) | [Network](#) | [Logs](#) | [SSL Certificate](#) | [Accounts](#) | [Console](#) | [Logout](#)

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

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

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):

Country Name:

State or Province Name (eg, Florida):

Locality Name (eg, Miami):

Organization Name (eg, Miami Field Services Inc):

Organizational Unit Name (eg, Engineering):

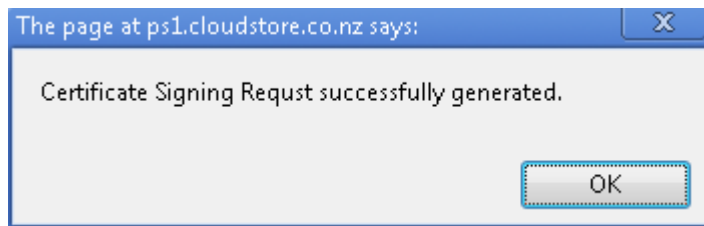
Common Name (eg, the Fully Qualified Domain Name you have given to this Private Server for example: getconsole.miamifieldservices.com):

Email Address:

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.

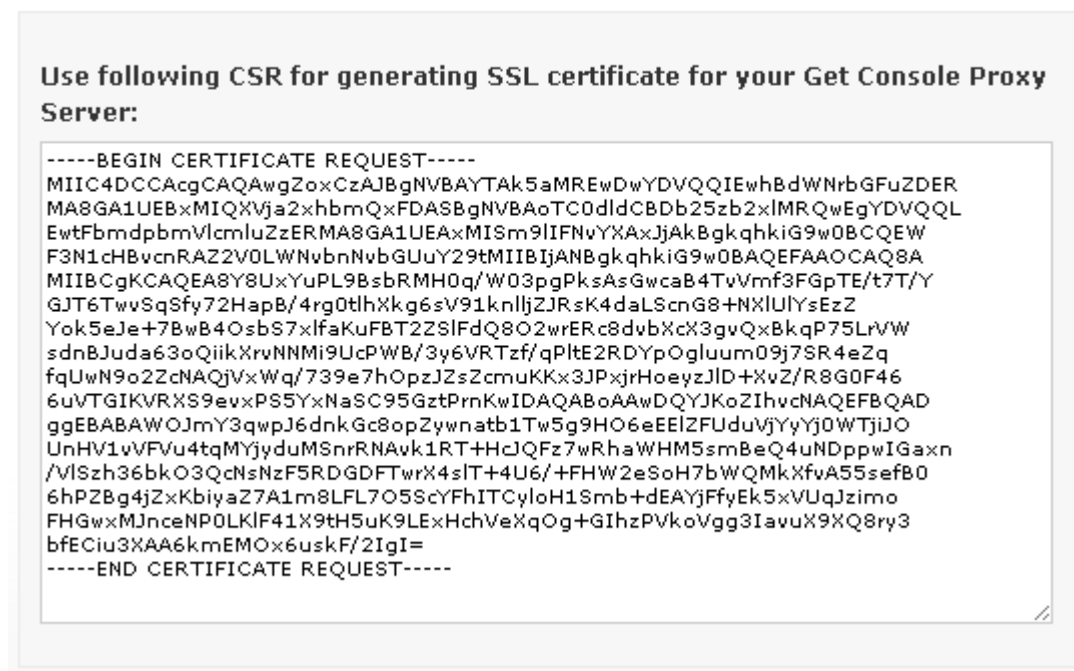
Once this form has been filled in correctly a message will be displayed that the Certificate Signing Request has been successfully generated. Click OK



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.

The in-the-field Apple iOS devices will now be able to use the “Secure Connection” 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 1.2, the Virtual Appliance and Database files can be updated without re-installing the Virtual Appliance. This feature will be used to non-destructively update Private Servers from version 1.2 to version 1.3 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.

AUTOMATIC UPDATES

The Semi-Automatic update process involves checking the Get-Console.com website for new Private Server versions, if a new version exists downloading it and then if downloaded successfully, installing it. No restart of the Private Server is 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)

The screenshot shows the 'Private Server Web Manager' interface. At the top is a navigation bar with links: Home, Network, Files, SSL Certificate, Accounts, Console, and Logout. Below the navigation bar, under 'Update Options:', there are two options: '1. Update your Private Server automatically (Internet connection required)' and '2. Update your Private Server manually'. To the right, under 'Update Private Server:', it says 'To update your Private Server click [here](#)'.

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

This screenshot shows the 'Update Options -> Update your Private Server automatically (Internet connection required)' section. It includes a 'Check for updates:' section with a 'Submit' button. Below that, it states 'The latest Private Server version is 1.2.1'. Then, under 'Download Private Server update to version 1.2.1:', there is a 'Download Update 1.2.1:' section with a 'Submit' button. To the right, under 'Update Private Server:', it says 'To update your Private Server click [here](#)'. Below that, under 'Get Support:', it says 'Read the [User Manual](#)'. Then, 'See the Private Server FAQ [here](#)'. Then, 'Visit the Community Forum [here](#)'. Finally, under 'Our Contact Details:', it says 'Customers with a valid support contract can contact us at:'.

After downloading, the dialog box will allow for installing

This screenshot shows the 'Download Private Server update to version 1.2.1:' section. It includes a 'Download Update 1.2.1:' section with a 'Submit' button. Below that, it says 'Update file was downloaded successfully.'. Then, under 'Install Private Server version 1.2.1:', there is an 'Install update:' section with a 'Submit' button.

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:

Install update:

Submit**Update Log:**

```

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 is identical as the above automated process, except that the update zip file can be obtained from the www.get-console.com/download website offline, and then uploaded to the Private Server via selecting option 2



After uploading, click Submit button under the “Install update” heading and as per the automatic process the patch file will unzip and execute. The screen will show which files are changed and when the database has been successfully updated.

```

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.

```

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.
- 2) a valid username for a user defined on the Private Server must be entered into username field
- 3) the password for that Private Server hosted username must be entered correctly
- 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:

Remote Settings

Remote Server Private Server >

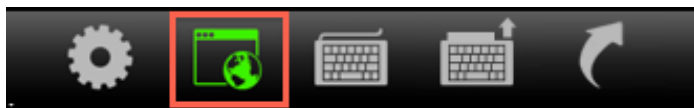
Private Server `ps1.cloudstore.co.nz` Set to the IP address or DNS name of your Private Server

Secure Connection enable secure connection only if a valid SSL Certificate has been installed on Private Server ON

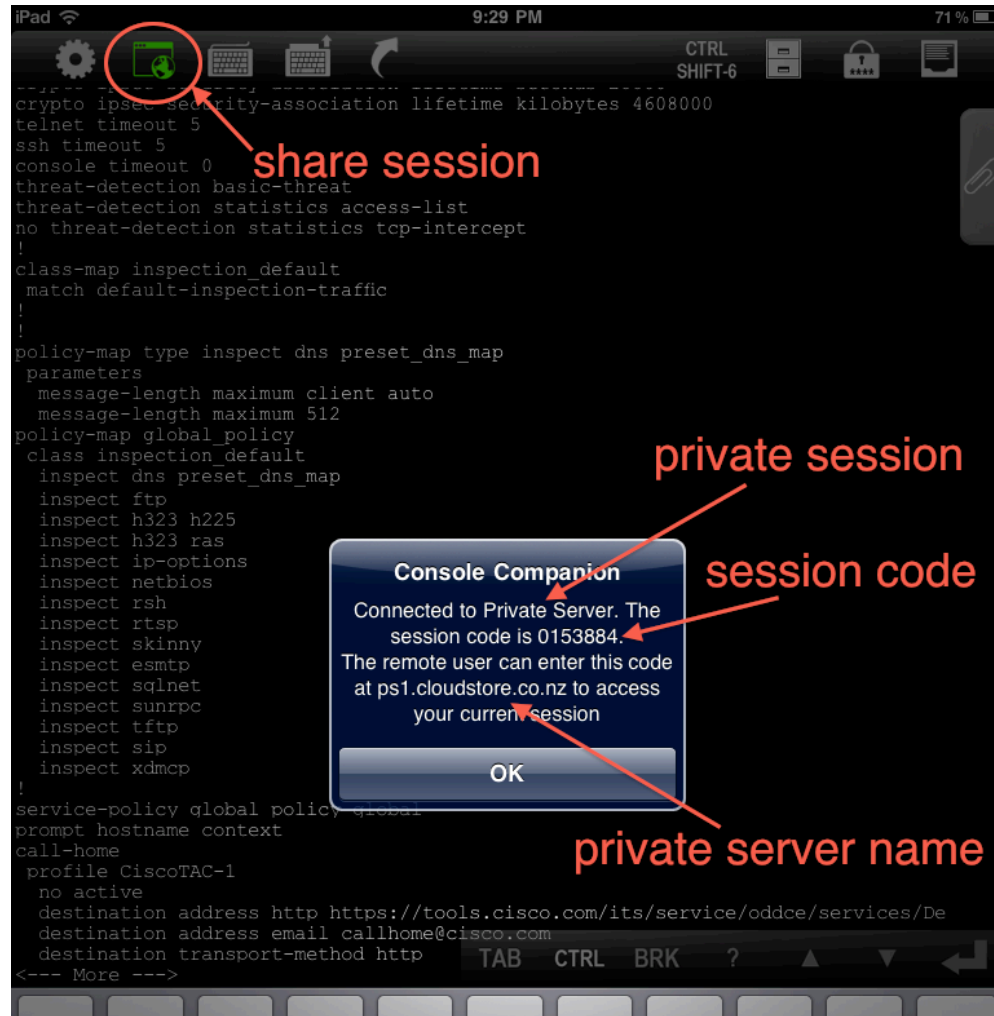
Username `simon` Set the username to a used defined on the private Server

Password Password for above username as defined in the Accounts section of the Private Server

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 remote PC user can now see the remote iOS device in the Private Server home page, and also in the Console page.

Private Server Web Manager

get console private server

Home Network Logs SSL Certificate Accounts Console Logout

Active Proxy Sessions:

Session Code	Remote Host	Device Name	Device System Model	Connected
0714005	115.189.129.158	Simon Hope's iPhone	iPhone	2011-04-29 17:09:31

Control keys... ps1.cloudstore.co.nz (Get Console Virtual Appliance) [close]

Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^['.
Session code:

The PC user can also use a generic telnet client to access to remote iOS device terminal session using port 2323.

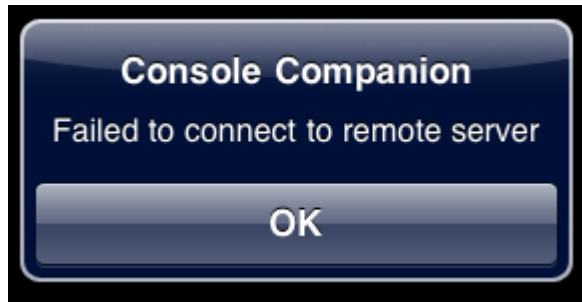
To use a third party telnet client rather than the web client, simply telnet to the Private Servers IP address (or domain name) on TCP port 2323. A session code prompt will be presented where the PC user can enter the code of the remote iOS device to be connected.

The Console page will allow the PC based user to access the console session of the remote iOS device.

Once you select this page you will be prompted for a session code, however simply clicking on one of the available session codes displayed above the console window will automatically enter the code and connect to the remote iOS device session.

TROUBLESHOOTING CONNECTIVITY TO PRIVATE SERVER

GENERAL CONNECTIVITY ISSUES

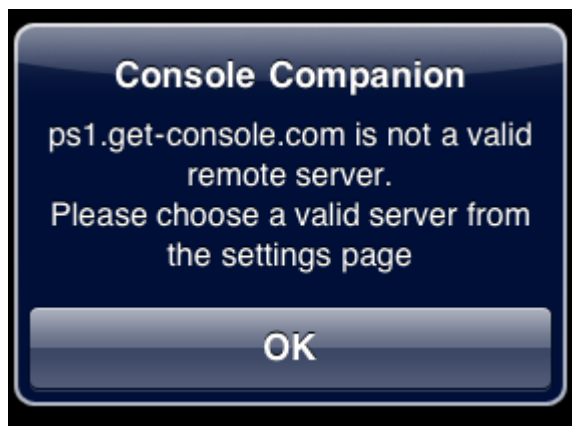


The above message will be displayed on the apple iOS device when:

- 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 not 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**

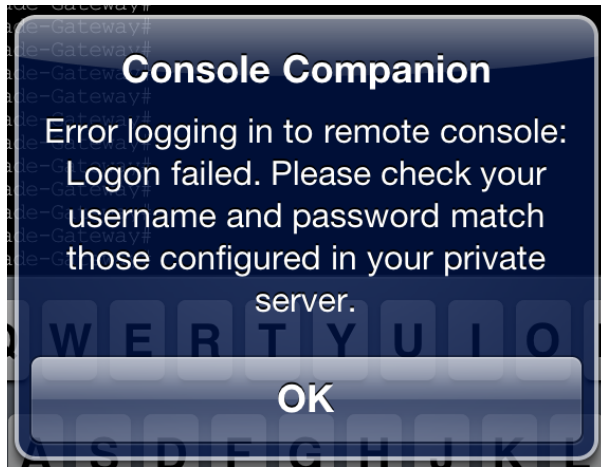
Please correct the connectivity issues for the iOS device or Private server, or disable “Secure Connection” in settings then try again.

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.

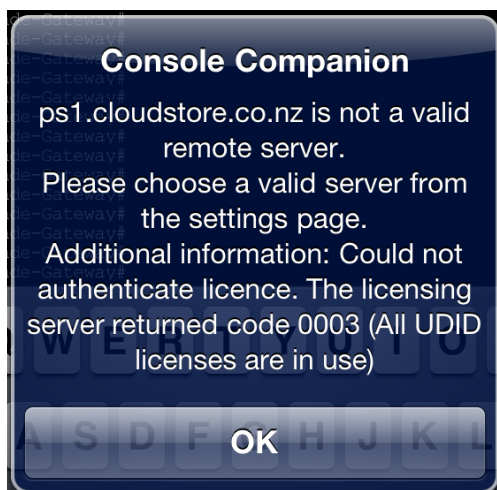
INCORRECT USERNAME OR PASSWORD



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

Note there is a lead time of 4 hours from purchase to upload the CAL license details to the license server.