Bringing a new Gallagher Controller online with Command Centre

Technical Information Paper

The complexity of IP networks can make bringing a Gallagher Controller online with the Command Centre server (specifically the Controller Service) a non-trivial process, and the best approach is dependent on the network (i.e., subnets, routing, firewalls, DHCP, DNS, NAT, VPN can all play a role).

Most networks should be able to be set up so powering on the Controller with only dipswitch 2 on [factory default] will work if the Controller is first configured correctly in Command Centre. A Controller Hardware Item with the matching MAC address and desired IP configuration must be added in the Command Centre Configuration client to allow the matching Controller to come online.

To establish connectivity with Command Center on an Ethernet network, the Controller must receive IP configuration for its own Ethernet Adapter and the IP or DNS name of the Command Centre Controller Service host with one of the following approaches.

Initial Connectivity approaches (v8.90+)

To bring a Controller online, one of the following approaches should be used in consultation with a network administrator. The following only applies to Controllers running v8.90 or later with Command Centre v8.90 or later. All 6000 and 7000 Controller have been produced with v9 software on them since December 2023. If installing a Controller that does not meet this criterion, read the "Earlier Controller Software versions" section first.

Any IP configuration provided by DHCP, Bootp service, or web configuration page will be overruled by the IP configuration in Command Centre once the Controller connects. A static IP approach can be used to get the Controller to initially connect to Command Centre, but the Controller can switch to automatic/DHCP once communication is established with Command Centre (if configured to do so) and vice versa.

Ensure the Command Centre Controller Hardware Item network configuration is correct – particularly the MAC Address, Server Address, and, if not using DHCP, the manual IP Address, Subnet Mask and Gateway – before attempting any of these approaches.

Notes:

- Remember to turn off dipswitch 1,2,3 & 4 once the Controller is online with Command Centre or this process may need to be repeated on a Controller restart (including software upgrade) or the Controller is left in an insecure state.
- The Controller usually requires outbound access to the Command Centre Controller Service host IP on port TCP/IP port 1072 for normal operation. Some approaches, but not all, allow an alternative port number to be used, although this can be changed once the Controller is online. The Command Centre Controller Service host IP only requires downstream access to the Controller on port TCP/IP port 1072 to perform the 'Send Server Address' override [NAT would require port forwarding], which is not required for general operation and only useful in a few of the below connectivity approaches.

1. Controller uses generic DHCP and finds server with 'gallagherserver' DNS lookup

Note: This may not be viable if multiple Command Centre Servers exist on the network, and DNS cannot be set up to direct the appropriate Controllers to their respective server IP.

Dipswitch 2 should be on, dipswitch 3 & 4 off when powering on the Controller, ethernet connected to network.

Network Administration must ensure generic DHCP support on the network will allocate an IP to the Controller, the 'gallagherserver' DNS lookup resolves to the Command Centre Controller Service host IP and the Controller must be able to reach upstream via TCP/IP to 'gallagherserver' address on port 1072.

Neither the Command Centre Bootp Service nor custom DHCP configuration are required but will still be accepted by the Controller. If both generic DHCP and Bootp/custom DHCP are operating, the service that responds to the Controller fastest will determine the Controller IP resulting in inconsistent behaviour.

2. Controller uses Command Centre Bootp Service customised DHCP - similar to pre-v8.90 dipswitch 2 behaviour

Note: If the Controller is installed in a subnet different from that of the server or has a managed switch between them, then DHCP broadcasts are unlikely to be forwarded between the server and Controller without appropriate routing rules.

Dipswitch 2 and 4 should be on, dipswitch 3 off when powering on the Controller, ethernet connected to network. Dipswitch 4 is only required in v8.90+ to ignore Generic DHCP responses, so this approach will function with the factory default dipswitch setting if DHCP is not present on the network.

The Command Centre Bootp Service must be online and able to receive (ipv4 port 68) and send DHCP responses (ipv4 port 67) to the Controller location. Controller must be able to reach upstream to the server IP on TCP/IP port 1072, downstream is not required.

The Command Centre Bootp Service will send some of the manual IP configuration [IP Address, Subnet, Gateway and server IP/Name] from the Command Centre Controller Hardware Item so the item must be configured with correct manual network configuration before DHCP responses will succeed. The IP configuration sent to the Controller is recorded in "The configured IP address ...sent to the Controller" events which can be inspected to confirm the correct details have been sent to the Controller .

3. Controller configured with static IP Configuration and Server IP/DNS setup via Controller webpage directly connected to laptop

Dipswitch 1, 2 and 3 should be on, dipswitch 4 off when powering on the Controller.

The Controllers Ethernet can be connected to laptop/PC directly with cross over or patch cable or indirectly with an unmanaged switch. Some laptops have experienced issues with a direct patch cable connection which can be worked around via forcing full duplex and/or 10Mbps speed options on the laptop ethernet adaptor. Once configured correctly the Controller can be transported and connected to the destination network with or without power.

Neither the Command Centre Bootp Service, custom DNS entries nor custom DHCP configuration are required.

The Controller can be configured on site and cables swapped after web configuration or off site and moved to installation location without power. Refer to the appropriate *Controller Installation Note* for the full process.

Controller must be able to reach upstream to server IP/DNS on configured port [not restricted to port 1072], downstream from Command Centre is not required.

4. Controller uses customised DHCP responses from existing network DHCP service

Dipswitch 2 and 4 should be on, dipswitch 3 off when powering on the Controller, ethernet connected to network. Dipswitch 4 is only required in v8.90+ to ignore Generic DHCP responses, so this approach will function with the factory default dipswitch setting if Generic DHCP is not present on the network.

Command Centre Bootp Service is replaced by the network DHCP service and should be disabled. Custom DNS entries are not required.

The Network Administrator must customize their DHCP service responses to include the Command Centre Controller Service IP/DNS name inside compatible vendor encapsulated options. Refer to *DHCP Server Configuration.pdf* for detailed instructions in the 'Utilities\DHCP' directory of the Command Centre installation files.

The DHCP Service must be able to receive (ipv4 port 68) and send DHCP responses (ipv4 port 67) to the Controller location including the customized response content. The Controller must be able to reach upstream to the server IP on TCP/IP port 1072.

5. Controller uses generic DHCP, and server IP configuration sent from Command Centre with 'Send Server Address' override

Dipswitch 2 should be on, dipswitch 3 & 4 off when powering on the Controller, ethernet connected to network.

The Network Administrator must provide some means (network dependent - not specified by Gallagher) to determine the IP address allocated to a Controller. The Controller may use the hostname "C6000" or “C7000” for DHCP requests so DHCP logs or automatic DNS entries may be useful.

The allocated IP address must be configured in Command Centre then the 'Send Server Address' override should be performed. The Command Centre Controller Service must be able to reach downstream to the Controller on TCP/IP port 1072 only to perform the override, downstream port access not required once online. Once the override succeeds the Controller will connect upstream to the server IP/DNS on the configured port (not restricted to port 1072).

Neither the Command Centre Bootp Service nor custom DHCP configuration are required but will still be accepted by the Controller. If both generic DHCP and Bootp/custom DHCP are operating, the service that responds to the Controller fastest will determine the Controller IP resulting in inconsistent behaviour.

6. Controller uses generic DHCP then Server IP/DNS setup via Controller webpage

Dipswitch 1 & 2 should be on, dipswitch 3 & 4 off when powering on the Controller, ethernet connected to network.

The Network Administrator must provide some means (network dependent - not specified by Gallagher) to determine the IP address allocated to a Controller. The Controller may use the hostname "C6000" or “C7000” for DHCP requests so DHCP logs or automatic DNS entries may be useful.

The Controllers network configuration webpage allows Controller IP and Server configuration to be specified via any PC/Laptop on the network able to access it on TCP/IP port 80. Refer to the appropriate *Controller Installation Note* for the full process.
Once configured the Controller will connect upstream to the server IP/DNS on the configured port (not restricted to port 1072).

Neither the Command Centre Bootp Service nor custom DHCP configuration are required but will still be accepted by the Controller. If both generic DHCP and Bootp/custom DHCP are operating, the service that responds to the Controller fastest will determine the Controller IP resulting in inconsistent behaviour.

7. Connecting Controller 7000s to Command Centre via OneLink

This functionality requires Command Centre 9.30+ connected to the Gallagher Cloud and an active Sales & Maintenance Agreement/Care Plan.

The Controller must have an item created for it in Command Centre with 'OneLink' selected for network connectivity with the correct MAC address and correct Serial Number from the Controller's packaging/ stickers configured. The item network configuration page will register the Controller for OneLink - this registration must be refreshed if it expires before the controller establishes the initial connection.

The Controller software version must be 9.30+ this may be indicated on the packaging for recently manufactured controllers, otherwise the controller must be upgraded via Command Centre before it is OneLink capable

To connect a Controller to Command Centre via OneLink for the first time it should be powered on with dipswitches 2 and 7 turned on (all other dipswitches must be off). The Controller must be connected to a network that will provide DHCP, DNS and outgoing TCP connections to *.gallagher.cloud internet locations on ports 80 and 443. No incoming connections from the internet are required and a firewall is recommended to stop incoming connections. Once the Controller has established connection to Command Centre (visible from Controller status page) and the Run LED is in a consistent single flash state dipswitch 2 and 7 should be turned off.

If this process is reattempted with the same Command Centre Controller item and Controller the dipswitches 2 and 7 will need to be turned on again, the OneLink registration of the Command Centre Controller Item may need refreshing, and the revalidate certificate override is required. Reattempting this process is not required to move the controller between two network locations that both allow internet access.

Controller cryptographic restrictions and moving/replacing Controllers

Each Controller has a pre-programmed unique Ethernet address (MAC address) which is used to identify Controllers during cryptographic authentication. Controllers without a MAC address matching a configured MAC address on the Controller Hardware Item, network devices not supporting the Command Centre/Controller protocol or missing the cryptographic keys and certificates needed for the respective MAC address will not be allowed to communicate with Command Centre.

Once online, the Command Centre Controller Hardware item and Controller will be cryptographically bound with new keys and certificates generated for that connection; blocking any other Controller connecting to that Command Centre Controller Hardware item or any other server configuring the Controller.

The Command Centre Controller Hardware item will lose its association to the Controller when a 'Revalidate Certificate' override is performed and allow a new [MAC address updated to match] or existing Controller to connect.

The Controller will lose its association to the Command Centre Controller Hardware item when powered on with dipswitch 2 on and will allow establishing a connection to a new Server but cannot connect to the same server Command Centre Controller item unless a 'Revalidate Certificate' override is performed to allow new generated certificates to be bound. If any of the Initial Connectivity Approaches are used again to move a Controller to a new network location the 'Revalidate Certificate' override must be performed.

If anyone accessed the Controller and repowered it with dipswitch 2 on to attempt reconfiguring it (potentially with another server) the server will raise offline alarms when the Controller doesn't respond and if the Controller attempts to connect back again it will raise authentication failed alarms. If these alarms occur and a dipswitch 2 on restart of the Controller is not expected it should be investigated.

An online Controller can be reconfigured in Command Centre for network configuration for a new location network so dipswitch 2 changes are not required but if that IP configuration is not valid for its current location it may not come back online until moved.

Earlier Controller Software versions

The above approaches may not work on Controllers running 8.80 software or earlier.

- Controller 7000 Single Doors were distributed with earlier software [update ETA late 2023].
- Controller 6000s were distributed with earlier software prior to September 2023.
- Controller 6000s since September 2023 that are factory reset (via dipswitch 8) return to an 8.40 version for older site compatibility.
- Controllers that have been installed on a Command Centre site previously may have been downgraded.
- Controllers running v8.80 or earlier: Generic DHCP support is not present.
- Controllers running v8.40 or earlier: An older TCP/IP protocol is used that required both upstream and downstream connections between Command Centre and the Controller for normal operation. The v8.50+ Command Centre Controller Service must be able to reach downstream to the Controller via TCP/IP port 1072 to establish both connections to Controllers using the earlier protocol to communicate and allow upgrading of the Controller. Check the network Firewall and routing configuration to allow these Controllers to connect to Command Centre.
- Controllers running 8.30 or earlier: The Controller is not able to receive configuration from 8.40+ Command Centre until upgraded - dipswitch 2 should remain on until upgraded which may require the Controller to brought online again after installing updated software.

The most reliable way to determine the version of a Controller that is not configured on Command Centre is via the web interface - see approach 3 and look for the Version details at the bottom of the web page.

The approaches that do not use generic DHCP are available on Controllers with earlier software:

- 2. Controller uses Command Centre Bootp Service customized DHCP [classic pre-8.90 dipswitch 2 behaviour].
  Note: Dipswitch 4 must be off on earlier Controller software versions for this to function.
- 3. Controller configured with static IP Configuration and Server IP/DNS setup via Controller webpage.
- 4. Controller uses customized DHCP responses from existing network DHCP service.

Earlier Command Centre versions

Compatibility between different versions of Command Centre and Controller software has changed as protocol changes have been required. Command Centre v8.70+ is required for Controller 7000 Single Door support and Command Centre v9.00+ for the Controller 7000 Standard.

Command Centre v8.50 to 8.80

All options to bring the Controller 6000 online will work but there is no support for generic DHCP once the Controller has come online with Command Centre so customized DHCP or static IP must be configured.

Command Centre v8.20 to 8.40

Only v8.50+ Command Centre can communicate to v8.50+ Controller software; this is due to the migration of the Controller to a Websocket based protocol that only required an upstream connection to the server in v8.50 onwards. Prior to 8.50 the Command Centre and Controllers needed to establish TCP/IP port 1072 connections in each direction.

For this reason, all Controller 6000s released with v8.90+ software will return to v8.40 software upon a factory reset to allow installation on v8.20-8.50 versions of Command Centre. To bring a recently produced Controller 6000 online with v8.20-8.50 Command Centre you will need to perform the factory reset (dipswitch 8) procedure. Note that the reset to v8.40 removes the support for generic DHCP approaches (see "Earlier Controller Software versions" section) and can only be reversed by bringing the Controller online with Command Centre and upgrading back to v8.90.

Command Centre v7.00 to 8.10

Command Centre Command Centre versions prior to v8.20 need upgrading before newly manufactured Controller 6000s can be installed. The Controller software changed to a Linux based operating system in v8.20 breaking compatibility with earlier Command Centre versions.