# Table of Contents

1  **Introduction to Accelerator** ................................................................. 4  
   1.1  Introduction ....................................................................................... 4  
   1.2  Technical Architecture ...................................................................... 5  
      1.2.1  Registration Process of Accelerator Node ................................. 5  
      1.2.2  Attendee’s Join Flow ................................................................. 6  
   1.3  Accelerator Security Aspects ............................................................. 6  

2  **Accelerator VM Specifications & Prerequisite** .................................... 7  
   2.1  Accelerator VM Specifications .......................................................... 7  
   2.2  Accelerator Deployment Prerequisites ............................................. 7  
   2.3  Network & firewall Configuration Recommendations ........................ 8  

3  **Accelerator Setup Instructions** .......................................................... 9  
   3.1  Generate Pairing Code ..................................................................... 9  
   3.2  Deploy Accelerator Virtual Machine ............................................... 11  
      3.2.1  OVF/OVA deployment ............................................................... 11  
   3.3  Configure Accelerator ...................................................................... 15  
   3.4  Check Deployed Node Status ......................................................... 19  
   3.5  Check Feature Enablement by Enterprise Admin ............................. 20  

4  **Manage Accelerator via Node Console** ................................................ 21  
   4.1  Introduction ....................................................................................... 22  
   4.2  Main Menu ......................................................................................... 22  
      4.2.1  Manage Network Settings ....................................................... 23  
      4.2.2  View Registration Status ....................................................... 25  
      4.2.3  Change Password .................................................................... 25  
      4.2.4  SSL settings ........................................................................... 26  
      4.2.5  Proxy Settings ......................................................................... 26  
      4.2.6  NTP settings ........................................................................... 29  
      4.2.7  Uninstall the Configuration ..................................................... 30  
      4.2.8  Reboot ..................................................................................... 31  
      4.2.9  Custom SSL Proxy Settings ...................................................... 32  

5  **Manage Accelerator via SSH to Node Console** .................................... 34  
   5.1  Introduction ....................................................................................... 34  
   5.2  New Node Installation ..................................................................... 34  
   5.3  Upgraded Node ................................................................................. 35  

6  **Manage Accelerator via Enterprise Admin on BlueJeans Cloud** ............. 36  
   6.1  Introduction ....................................................................................... 36  
   6.2  View Accelerator Nodes of Enterprise ........................................... 36  
      6.2.1  View Node Specific Information Name ..................................... 38  
   6.3  **Modify Accelerator Node configuration** ........................................ 39  
      6.3.1  Modify Node Name ................................................................... 39  
      6.3.2  Add/Modify Public IPs ............................................................... 40  
      6.3.3  Enable/Disable draining of a Node .......................................... 41  
   6.4  **Remove Node** ............................................................................. 42  

© 2018 BlueJeans Network
7 Centralized Internet........................................................................................................44
  7.1 Introduction ..................................................................................................................44
  7.2 Know Your Setup .........................................................................................................44
    7.2.1 Decentralized Internet Network ...........................................................................44
    7.2.2 Centralized Internet Network ..............................................................................45
    7.2.3 Hybrid Network .....................................................................................................46
  7.3 Centralized Internet Nodes Configuration ....................................................................48
    7.3.1 Configuration concepts with example ....................................................................48
    7.3.2 Configure Private Network Address via Admin Portal ........................................49
8 HTML5 support on Accelerator .........................................................................................51
  8.1 Introduction ..................................................................................................................51
  8.2 Prerequisites .................................................................................................................51
  8.3 Certificate Provisioning .................................................................................................52
  8.4 Steps for configuring Accelerator for HTML5 support ................................................53
  8.5 Simplified Certificate Provisioning ..............................................................................58
    8.5.1 Benefits of Simplified Provisioning ......................................................................58
9 Annexures ........................................................................................................................59
  9.1 Annexure 1: Generate self-signed certificate ...............................................................59
    9.1.1 Steps to Generate Certificate ..............................................................................59
1 Introduction to Accelerator

- Introduction
- Technical Architecture
- Accelerator Security Aspects

1.1 Introduction

BlueJeans Accelerator is a product deployed within an enterprise network which helps optimize the WAN bandwidth consumption when a Primetime event is streamed to a large number of attendees within an enterprise. This Accelerator fetches the Primetime media streams from the cloud, caches the media chunks and serves the clients locally.
1.2 Technical Architecture

1.2.1 Registration Process of Accelerator Node

On deployment of an Accelerator node in an enterprise, it tries to connect with the BlueJeans cloud to send registration message comprising of: Pairing code (for Authentication), Private IP Address (Internal IP Address of Accelerator configured by admin), Version no. etc.

BlueJeans Cloud Service maintains private IP & public IP mapping of all the registered Accelerator nodes. BlueJeans cloud service picks private IP address from registration message of Accelerator node and maps it with the public IP fetched from the Source IP address of the request.

This public & private IP mapping is maintained in a BlueJeans Database which is used to identify nodes deployed at specific enterprise office and can later be mapped with Attendees who are streaming from the same office.
1.2.2 Attendee’s Join Flow

On entering attendee URL on the Browser, HTTPS request is sent to BlueJeans Cloud. Based on the attendee’s URL, BlueJeans cloud checks for the enterprise and On-Prem enablement.

If On-Prem is enabled for that enterprise and deployed Accelerator is in “Online” state, then BlueJeans Cloud will reply with the URL comprising the Internal IP address of the Accelerator node.

Now attendee requests for the stream directly from the Accelerator node deployed within its enterprise using the Internal IP of Accelerator Node.

Once Accelerator gets the Attendee request, it starts fetching the stream of the event from the nearest CDN server and start caching it. All the attendees who are streaming the Event from the same Enterprise Office will fetch the stream from the Accelerator directly.

1.3 Accelerator Security Aspects

Accelerator uses “Pairing code authentication” at the time of installation of node. This is a secure & reliable way of authenticating any Accelerator node deployed at any Enterprise with BlueJeans Cloud. Pairing code is an alphanumeric key generated by BlueJeans and it can be used only once for registration and can’t be used again, even for the same node.

Accelerator receives the Stream from CDN over https, therefore all the communication between Accelerator and CDN is secure. In case of Accelerator Nodes failure, Attendees fetch the stream from CDN over HTTPS.

NOTE: The Accelerator makes HTTPS requests to the BlueJeans cloud infrastructure over port 443. The enterprise admins should ensure that these ports are not blocked in the outbound direction. Therefore no inbound firewall ports need to be opened. Strongly recommend to deploy Accelerator Node in trusted/Inside Zone and not in DMZ or untrusted zone.
2 Accelerator VM Specifications & Prerequisite

- Accelerator VM Specifications
- Accelerator Deployment Prerequisite
- Network & Firewall Configuration Recommendations

2.1 Accelerator VM Specifications

The product is delivered as a Virtual Machine software.

Each VM is shipped with following pre-configured settings:
- 2 vCPUs
- 4GB Memory
- 20 GB HDD
- VMXNET 3 Network Adapter for OVF/OVA image

------------------------------------------------------------------------------------------------------------

NOTE: Please retain these settings and assign a minimum of 1Gbps NIC to each Accelerator. Modifying these settings can impact Accelerator performance.

------------------------------------------------------------------------------------------------------------

2.2 Accelerator Deployment Prerequisites

Accelerator deployment prerequisites are as follows:

1. Accelerator software is available as Virtual Machine image in the following formats:
   - OVF
   - OVA
   - HyperV
   Please download the appropriate image

2. Software Requirement:
   - OVF/OVA deployment is qualified with VMware ESXi versions 5.5 & 5.10.

3. Hardware Requirement: Supporting any standard x86-64 server running at minimum 2.5 Gh

4. One IP Address on the local network (which Admin can assign to Accelerator)
5. One Pairing Code generated on the BlueJeans Enterprise Admin page (to register & authenticate Accelerator with BlueJeans Cloud)

6. 1 Gbps dedicated NIC for each Accelerator.

### 2.3 Network & firewall Configuration Recommendations

1. The Accelerator is a device on the LAN. It should be accessible by local endpoints over the LAN. Strongly recommended to deploy Accelerator Node in trusted/Inside Zone and not in DMZ or untrusted zone.

2. In addition, it needs Internet connectivity to the BlueJeans cloud infrastructure.

3. The Accelerator makes HTTPS requests to the BlueJeans cloud infrastructure over port 443. The enterprise admins should ensure that these ports are not blocked in the outbound direction on Firewall.

4. In case all domains on port 443 are not allowed by default and only selected sites are allowed, then make sure the following domains are whitelisted:
   - bluejeans.com
   - a2m.bluejeans.com
   - tracker.bluejeans.com
   - primetime.bluejeans.com
   - streaming.bluejeans.com
   - streaming-akamai.bluejeans.com
   - ull-streaming-akamai.bluejeans.com
   - bjnsecure_z-vh.akamaihd.net
   - accelerator-update.bluejeans.com
   - accelerator-coreos-updates.bluejeans.com
   - quay.io
   - cdn.quay.io
   - cdn01.quay.io
   - cdn02.quay.io
   - cdn03.quay.io
   - quay-registry.s3.amazonaws.com
   - *.pubnub.com
   - *.pndsn.com
   - *.pubnub.net
   - *.pubnub.io
   - *.cloudfront.net
   - *.sumologic.com
   - *.flatcar.pool.ntp.org
3 Accelerator Setup Instructions

- Generate Pairing Code
- Deploy Accelerator Virtual Machine
- Configure Accelerator
- Check Deployed Node Status

3.1 Generate Pairing Code

The steps below will help you to generate Pairing Code which you can use to register & authenticate Accelerator with BlueJeans.

1. Login to your BlueJeans account by using your Enterprise Username & Password at URL: https://bluejeans.com

2. Once you access your account then navigate to Admin -> Manage Accelerator.

3. Click on “+Add Node” button.

4. Enter Name in the field. (Note: - This Name is for your reference to manage these nodes therefore give names which will help you to recognize these nodes. For e.g. you can mention Lab, IP, Location etc. here.)

5. Once Name is provided then click on “Save” Button.
6. Note down this Pairing Code. You will need this pairing code when you deploy the Accelerator VM in section 3.3.
3.2 Deploy Accelerator Virtual Machine

3.2.1 OVF/OVA deployment

This section will guide you on how to deploy Accelerator OVF/OVA image in enterprise Network

1. Download the On-Prem Accelerator VM Package “BlueJeans_Accelerator_V5.8” from BlueJeans shared site.

2. Open VSphere Client and here select File → Deploy OVF template.

3. Then browse to the folder where you extracted the files and you should see a BlueJeans_Accelerator_V5.8.ovf file, select that and click “Next”.
4. Select Next for the “OVF Template Details”

5. Enter a descriptive name for this VM Node and select “Next”.
6. Choose Destination Storage by selecting appropriate datastore and select “Next”.

7. Select Disk Format “Thick Provision Lazy Zeroed” or “Thin Provision” based on disk space management and utilization as per your enterprise policy & practice and then select Next.

8. Then map the network used in this OVF template to network in your inventory by selecting drop down menu (if more networks are configured) under Destination Network and select Next.

9. Review the summary and click on “Finish”. This will deploy the Accelerator on ESXi Hypervisor.

10. After deployment select your VM and click on edit settings. Make sure all the settings including VM's SCSI Controller, Hard disk and Network adapter settings should be adjusted according to respective setups.
11. Power on the BlueJeans Accelerator VM. For this first select it in the VM list and then right click to select Power-> Power On option.

12. Once the VM is powered ON then navigate to “Console” Tab to start configuration.

13. Click on the console Tab to enter into the console screen.
3.3 Configure Accelerator

This section will guide you how to configure following:-

- Network settings
- Registering Using Pairing Code

1. Open the console to the VM and login.
2. Using default username “core” and password “core123”.
3. Now admin should change to new Password and confirm it by re-entering it.

```
OnPrem Virtual Machine Setup Wizard
[Version: 5.8]
```
```
Please change the password for core
New password: _
```

---

**NOTE:** Please provide strong password with more than 5 characters and should comprise of upper and lower case letters and numeric characters. Password restriction is not enforced.

---

1. Configure following Network Settings:
   - IP Address : provide internal IP
   - Subnet Mask
   - Default Gateway
   - Primary DNS IP
   - Secondary DNS IP (this is optional and you can skip it by pressing Enter key)
Here, system shows configured information and ask for confirmation to save it. Type “y” and press Enter key for saving these settings.

2. Here system shows option to setup Web Proxy.
   Note: This step is optional and can be skipped by opting “n” here.

Type “y” and press Enter key to configure web proxy. Here Admin can configure HTTP and HTTPS proxy. Following two formats are allowed to enter:

a) <protocol>://<proxy_ip>:<proxy_port>

b) <protocol>://<username>:<password>@<proxy_ip>:<proxy_port>
Format parameters:

- `<protocol>` - http or https
- `<proxy_ip>` - IP Address of Proxy
- `<proxy_port>` - Port Number of Proxy
- `<username>` - Username to access Proxy
- `<password>` - Password to access Proxy

**Do you want to setup web proxy? Please type (y/n)**

```
y
```

**Enter the HTTP proxy in either of below 2 formats and hit Enter:**

2) `<protocol>://<username>:<password>@<proxy_ip>:<proxy_port>` Ex: https://oa:be@192.168.1.1:3128

**Enter HTTP Proxy:** http://denimuser:denim123@10.5.9.118:3128

**Enter the HTTPS proxy in either of below 2 formats:**

2) `<protocol>://<username>:<password>@<proxy_ip>:<proxy_port>` Ex: https://oa:be@192.168.1.1:3128

**Enter HTTPS Proxy:** http://denimuser:denim123@10.5.9.118:3128

**NOTE:** Web Proxy option is in Beta Phase. Squid proxy is qualified in house with Accelerator.

3. Once all Network setting are configured and applied then Admin is prompted for pairing code.

```
-------------------------------
Generate Pairing code from bluejeans admin
-------------------------------
Enter the pairing code here
```

4. Here provide the Pairing Code which we have generated in section 3.1 and then press Enter key.

5. “Pairing Code” Accepted message is shown if you have entered valid pairing code and if your VM is reachable to BlueJeans Cloud for registering this Accelerator Node.
NOTE: In the following conditions Pairing Code acceptance will fail:

- If Accelerator cannot reach the BlueJeans cloud. (For this make sure that your Network setting are such that Accelerator has internet access and you should be able to ping bluejeans.com)
- If you are providing wrong/invalid Pairing Codes.
- If you are providing a Pairing Code that has already been used. (Pairing code can be used only once for registration and can’t be used again, even for the same node.)

6. Once you get the Pairing Code acceptance message then you will be asked to reboot the VM by pressing “Enter” key. Here press “Enter” key to initiate reboot and with this Accelerator deployment process will be over.

```
Generate Pairing code from bluejeans admin
-----------------------------------
Enter the pairing code here
KksUB.
Pairing code accepted!
Created symlink from /etc/systemd/system/multi-user.target.wants/optimus-manager.service to /etc/systemd/system/optimus-manager.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/optimus-logger.service to /etc/systemd/system/optimus-logger.service.

COMMANDS: Needs REBOOT, Press "Enter" to reboot...
```

7. After node comes up, login again using default username “core” and with new password. Here Main Menu will be shown. Wait for 30 minutes and then issue command “docker ps”, which will show shell prompt. Here issue command “docker ps” to show all the four applications with following names: “quay.io/bjnquay/optimus-manager”, “quay.io/bjnquay/optimus-logger”, “quay.io/bjnquay/optimus-proxy:X.Y.Z”, “quay.io/bjnquay/optimus-cache:A.B.C”. This signifies that all the applications of Accelerator are up.
All Application containers comes up within 30 Minutes from reboot time. After reboot, latest images are downloaded from BlueJeans Cloud infrastructure and start its services. Therefore all the application containers takes up to 30 minutes. This time is variable and based on the Internet and download speed.

### 3.4 Check Deployed Node Status

The steps below will help you to check the status of Node on Enterprise Admin UI.

Login as Enterprise Admin and navigate to Admin-> Manager Accelerator. Here check following values for deployed Node:

- Registered : “Yes”
- Pairing Code : “Paired”
- Status : “Online”
NOTE: Registered “Yes” and Pairing Code “Paired” confirms that pairing code used at the time of deployment is accepted and this node is registered a valid Accelerator node with BlueJeans cloud.

Status value shows the node’s state like Online / Disconnected / Drained / Overloaded. Make sure after deployment your node should be “Online” state. It takes ~30 min for a node to come online after deployment.

3.5 Check Feature Enablement by Enterprise Admin

Admin should make sure that Onprem Accelerator feature is enabled at enterprise level for all the Primetime events.

To enable this feature navigate to Admin-> Manager Accelerator and here use turn On the toggle button and click on “Update” button.
NOTE: Admin should make sure that “Enable onprem for enterprise” toggle button should be turned ON before any Primetime event, if they want attendees to stream via Onprem Accelerator, else all the attendees will stream via cloud directly.

Caveat: Make sure that Attendees who are joining outside office/campus where Accelerator is deployed should turn off full-tunnel VPN. This is very important, as we do not want outside attendees to stream via Accelerator deployed at office/campus. This can impact Attendee’s user experience. If full-tunnel VPN is used then, attendees get internal IP of the office and therefore eventually starts streaming via Accelerator, which is not the ideal solution for the Attendees who are streaming from outside. They should stream directly from BlueJeans cloud to get better user experience.

In case of Split-tunnel VPN no action needs be taken, as outside traffic will go directly to Internet and should not be routed via office/campus.

4 Manage Accelerator via Node Console

- Introduction
- Main Menu Options
- Manage Network Settings
- View Registration Status on Accelerator
- Change Password
- SSL Settings for HTML5 support
- Web Proxy Support

© 2018 BlueJeans Network
4.1 Introduction

This section is focused on helping the administrator manage deployed Accelerator nodes. This will help administrator to modify Network settings, Password, add SSL settings, reboot node and even uninstall the complete configuration of any node.

NOTE - After configuring Network settings, Admin can access Accelerator Node setting options via either VM Console using [core] or via SSH login with [onpremuser] and switch to [core].

4.2 Main Menu

After providing valid username and password, the Accelerator Main Menu is shown. This Menu give following options to Admin user:

1. Edit Network Settings
2. View registration status
3. Change Password
4. SSL settings
5. Proxy Settings
6. NTP Settings
7. Uninstall the configuration
8. Reboot
9. Custom SSL Proxy Settings
Admin can select any of above options to

4.2.1 Manage Network Settings

Admin can view/modify/manage Accelerator’s Network settings using first option on Main Menu.

To select option [1] Edit Network Settings.

Enter your Choice: 1

Selecting this option will display your current Network Configuration. Here if Admin want to edit these settings then type “y” and then Enter.
Here, admin can change any of the following Network Settings:

- IP Address: provide internal IP
- Subnet Mask
- Default Gateway
- Primary DNS IP
- Secondary DNS IP (this is optional and you can skip it by pressing Enter key)

Existing Network Configuration is shown and if you want to change any setting then type it else hit Enter to skip.

After modifying Network Settings, system will show configured information and then apply it and ask for Reboot. Here press “Enter” key to reboot the system.
4.2.2 View Registration Status

Admin can view the registration status of Accelerator Node by selecting second option on Main Menu.

To select option [2] View registration status

Enter your Choice: 2

This option shows the Registration Status, Pairing Code & Node ID of the Accelerator Node.

Note: Main Menu will show option “Register with Pairing Code” if Node is not registered.

4.2.3 Change Password

Admin can change the password of the Accelerator Node any time after the deployment by selecting third option from Main Menu.

To select option [3] Change Password

Enter your Choice: 3

Admin should change to new Password and confirm it by re-entering it.
NOTE: Please provide strong password with more than 5 characters and should comprise of upper and lower case letters and numeric characters. Password restriction is not enforced.

4.2.4 SSL settings

Accelerator support HTML5 players to stream via it. For Flash player no extra configuration on Accelerator is required but to support HTML5 Admin has to install SSL certificate on Accelerator.

Please refer Chapter 8 for more details on configuring HTML5 support on Accelerator.

4.2.5 Proxy Settings

Admin can view/modify/manage Accelerator’s Proxy settings using fifth option on Main Menu.

To select option [5] Proxy Settings.

Enter your Choice: 5

Here Admin can select following options:

- Select option [1] HTTP proxy settings, to view/edit HTTP Proxy Settings
- Select option [2] HTTPS proxy settings, to view/edit HTTPS Proxy Settings
- Select option [3] To go to Main Menu, for redirecting Admin to Main Menu

4.2.5.1 HTTP Proxy Settings

Select option [1] HTTP proxy settings. This will display existing HTTP Proxy configuration and provide options to edit and delete these settings.
Select option [1] Edit HTTP proxy settings, to modify HTTP Proxy Settings.

Here Admin can configure HTTP proxy. Following two formats are allowed to enter:

a) `<protocol>://<proxy_ip>:<proxy_port>`

b) `<protocol>://<username>:<password>@<proxy_ip>:<proxy_port>`

Format parameters:

- `<protocol>` - http or https
- `<proxy_ip>` - IP Address of Proxy
- `<proxy_port>` - Port Number of Proxy
- `<username>` - Username to access Proxy
- `<password>` - Password to access Proxy

Select option [2] Delete HTTP proxy settings, for deleting all HTTP proxy settings.

Select option [3] To go to Main Menu, for redirecting Admin to Main Menu.

### 4.2.5.2 HTTPS Proxy Settings

Select option [2] HTTPS proxy settings. This will display existing HTTPS Proxy configuration and provide options to edit and delete these settings.

Here Admin can configure HTTPS proxy. Following two formats are allowed to enter

   c)  <protocol>://<proxy_ip>:<proxy_port>
   d)  <protocol>://<username>:<password>@<proxy_ip>:<proxy_port>

Format parameters:

- <protocol> - http or https
- <proxy_ip> - IP Address of Proxy
- <proxy_port> - Port Number of Proxy
- <username> - Username to access Proxy
- <password> - Password to access Proxy

Select option [2] Delete HTTPS proxy settings, for deleting all HTTPS proxy settings.

Select option [3] To go to Main Menu, for redirecting Admin to Main Menu.

⚠️ The accelerator nodes will use http/https long polling, or websocket, which will keep the connection open to these domains *pndsn.com *pubnub.io, *pubnub.net,*pubnub.com. Long polling timeout on our side is 320 seconds, please make sure proxy is able to handle long polling requests.
4.2.6 NTP settings

Admin can view/modify/manage NTP settings using sixth option on Main Menu.


Enter your Choice: 6

```
Your NTP configuration

NTP Server List: []

Please select from menu

  NTP settings:
  [1] Edit NTP settings
  [2] Delete NTP settings
  [3] To go to Main menu

Enter your choice: _
```

Select option [1] Edit NTP settings, to modify NTP Settings. Here Admin can enter list of NTP Servers, separated by space.

```
Enter your choice: 1

Enter the list of ntp servers, separated by space. Ex: 0.pool.example.com 1.pool.example.com

Enter NTP servers: _
```

*Caveat:* Editing NTP settings overwrite old NTP servers settings.

Select option [2] Delete NTP Settings, for deleting all NTP settings.

Select option [3] To go to Main Menu, for redirecting Admin to Main Menu.
4.2.7 Uninstall the Configuration

Admin can uninstall the Accelerator Node’s configuration by removing Network settings and Pairing Code by selecting seventh option from Main Menu.

To select option [7] Change Password

Enter your Choice: 7

Admin should choose “y” to uninstall all the configuration of the Node and then press any key to reboot after uninstall successful message is displayed.

Caveat: Process for uninstallation of node, will reset both [onpremuser] and [core] user password to default password. This brings down the node and should be used with care.
4.2.8 Reboot

Admin can reboot Accelerator Node by selecting eighth option from Main Menu.

To select option [8] Reboot

Enter your Choice: 8

Admin should select “y” to reboot Accelerator.
4.2.9 Custom SSL Proxy Settings

In order to be able to do deep packet inspection, i.e. decrypt all the traffic flowing via proxy, accelerator needs to trust the self-signed certificate used by your proxy server. Admin can modify/manage Accelerator's Proxy Server's certificate using ninth option on Main Menu.

To select option [9] Custom SSL Proxy Settings

Here, Admin can select following options:
• Select option [1] Edit cert settings, to edit the certificate
• Select option [2] Delete cert settings, to delete the certificate
• Select option [3] To go to Main Menu, for redirecting Admin to Main Menu

After pasting the certificate, wait for a couple of seconds. Certificate will be added to the trust store and Admin will be taken out of that screen. Reboot the machine as instructed in order to make those changes take effect.

Once rebooted, Accelerator is all set up to stream the event. Not only you will see the calls flowing through the configured proxy but you should also be able to decrypt the HTTPS calls.
5 Manage Accelerator via SSH to Node Console

5.1 Introduction

This section is focused on helping administrator to access Accelerator Node using SSH console. It provides details to use SSH for a new Accelerator Node installation and for already existing Accelerator Node.

5.2 New Node Installation

After the Accelerator Node is setup and configured, we can use SSH console and follow these instructions to manage accelerator:

1- Login to your Accelerator Node using [onpremuser] and default password [onrem123].

```
ssh onpremuser@XX.XX.XX.XXXX
```

2- After login, the system will force the user to change the password of [onpremuser] and from next time, user is required to login with the new password.

3- To make any modification into accelerator node and to get Main Menu options, you need to login into [core].

4- To login into [core] use “su – core” command and most recent [core] password.

```
onpremuser@localhost ~ $ su – core
Password: 
```
5.3 Upgraded Node

This Section is focused on helping administrator to access Accelerator Node and Menu Options using SSH console when the node is upgraded to the latest version:

1- SSH Terminal logging with/as [core] user will be disabled. Now you have to login SSH Terminal with/as [onpremuser].

2- Login to your Accelerator Node using [onpremuser] and default password [onprem123].

3- After login, the system will force the user to change the password of [onpremuser] and from next time, user is required to login with the new password.

4- To make any modification into accelerator node and to get Main Menu options, you need to login into [core].

5- To login into [core] use “su – core” command and most recent [core] password.

**NOTE**: After accelerator is upgraded, there will be an automatic restart however it doesn't restart while it's handling an active event. With each unsuccessful login attempts there will be login delay.
6 Manage Accelerator via Enterprise Admin on BlueJeans Cloud

- Introduction
- View Accelerator Nodes of Enterprise
- Modify Accelerator Node Configuration
- Remove Node

6.1 Introduction

This section is focused on helping administrator to view and manage an already deployed Accelerator Nodes on BlueJeans Network cloud.

This will help Admin to modify already configured Node's Name & also allow admin to add/modify Public IPs of Enterprise.

6.2 View Accelerator Nodes of Enterprise

To view and manage Node on BlueJeans Cloud follow these instructions: -

1. Login to your BlueJeans account by using your Enterprise Username & Password at URL: https://bluejeans.com

2. Once you access your account then navigate to Admin -> Manage Accelerator.

3. All the nodes deployed in an enterprise is displayed here.
Here following fields for each node are shown:

- **Name** : Specifies node name
- **Registered** : Values – Yes/No
  Indicate that Accelerator node is registered or not.
- **Pairing Code** : Values – alpha numeric value(Pairing Code) / paired
  Indicate that this node is paired or not.
  The pairing code is only shown when the node has not been paired.
- **Status** : Shows Node status and can have value:
  - **Online** – when node is UP and connected
  - **Disconnected** - when node is Down/Disconnected
  - **Draining** – when Admin drained this node.
  - **Overloaded** – when node is overloaded i.e. CPU utilization/memory usage/ bandwidth usage is more than 75%)
- **Edit Icon** : Allows Admin to edit the node settings.
6.2.1 View Node Specific Information Name

To view Node specific information follow these instructions:

- Click on Edit icon of any node.
- This will open a new page displaying all the Accelerator node information.

Here following fields for each node are shown:

- **Name**: specifies node name
- **Public IP Address**: shows Public IPs
  Note: First Public IP is auto populated at the time of registration. Admin can add more Public IPs based on their Network setup and requirement.
- **Internal IP Address**: shows Internal IP address specified by Admin at the time of deployment.
• **Available Bandwidth** : shows available bandwidth of any node (in Mbps).

• **Status** : shows Node status and can have value:
  - **Online** – when node is UP and connected
  - **Disconnected** - when node is Down/Disconnected
  - **Draining** – when Admin drained this node.
  - **Overloaded** – when node is overloaded i.e. CPU utilization/memory usage/bandwidth usage is more than 75%

• **Draining** : shows draining status.

### 6.3 Modify Accelerator Node configuration

Admin is allowed to modify only following four values and rest all are read only:
- Name
- Public IP Address
- Draining
- Centralized Internet : Private Network Address (This topic is covered in Chapter 7)

### 6.3.1 Modify Node Name

To modify Node name follow these instructions:

- Click on Edit icon of a node which you want to modify.

- This will open a new page displaying all the information of the Accelerator node.

- Here you can edit Name field.

- You can use any alphabet/number/special character in the Node name.

- Then click on “Save” button to save it.
6.3.2 Add/Modify Public IPs

To add/modify Public IP Address of a node follow these instructions:

- Click on Edit icon of a node which you want to modify.

- This will open a new page displaying all the information of the Accelerator node.

- Here you can add/modify Public IP Address of a node.

- Then click on “Save” button to save it.

Note: Give valid IP addresses. Admin can give multiple IP addresses separated by “,”. Admin can even mention network address in CIDR format.
6.3.3 Enable/Disable draining of a Node

To enable/disable Draining that allows the admin to stop streaming on that particular node without taking the accelerator node offline. To enable/disable Draining of a node follow these instructions:

- Click on Edit icon of a node which you want to modify.

- This will open a new page displaying all the information of the Accelerator node.

- Here Admin can switch ON/OFF the draining button by clicking on it. By default this option is disabled.

- Then click on “Save” button to save it.
Note: If user enable draining for a node and when that node is streaming the event then there will be no effect on active streaming but there will be no new streaming on that node until user disable draining.

6.4 Remove Node

Admin can remove any node from the list of the nodes installed in an enterprise. Follow these instructions to remove any node:

- Click on Edit icon of a node which you want to remove.
- This will open a new page displaying all the information of the Accelerator node.
- Here click on “Remove” button.
Caveat: Once any node is removed it can’t be recovered and Admin has to install that node again.
7 Centralized Internet

- Introduction
- Know Your Setup
- Centralized Internet Nodes Configuration

7.1 Introduction

This section is focused on helping administrator to understand different kind of networks where Accelerator can be deployed and configured.

This section is focused on configuring Centralized Internet Setup.

7.2 Know Your Setup

Admin should know their enterprise network/setup before deploying Accelerator nodes. Based on the Internet gateways in an enterprise, we have classified enterprise networks in following three categories:-

- Decentralized Internet
- Centralized Internet
- Hybrid Setup

7.2.1 Decentralized Internet Network

Decentralized internet networks have Internet gateway at each site from where Attendees will stream Primetime event. This means that all the attendees and Accelerator nodes deployed in these sites can access internet directly.

As each site has its own Public IP to connect Internet, therefore sites can be identified distinctly by BlueJeans cloud.
For such networks where all the sites in the enterprise have direct internet access, deploy Accelerator at each site and follow the deployment and configuration process mentioned in Chapter 3 and no extra configuration is required.

### 7.2.2 Centralized Internet Network

Centralized internet networks have Internet gateway at main site and rest all the sites are connected to main site to get Internet access. In this setup attendees and Accelerator nodes deployed at even sub sites are using the same Public IPs (of main site) to connect Internet.
In centralized internet setup if admin wants to deploy Accelerator nodes even at Sub sites, then first follow the basic deployment process mentioned in Chapter 3 and then configure centralized internet specific configuration. Please refer next section 7.3 to get more details about the Centralized Internet Configuration.

7.2.3 Hybrid Network

In Hybrid Network an enterprise can have multiple sites, where some sites have direct internet access and some are connected via Internet Gateway sites.
For Accelerator nodes deployed at decentralized sites, like nodes on Site1 & Site2 illustrated in above image, follow the basic deployment process mentioned in Chapter 3 and no extra configuration is required.

For Accelerator nodes deployed in centralized internet sites, like nodes on Main Site, SiteA & SiteB illustrated in above image, first follow the basic deployment process mentioned in Chapter 3 and then configure Centralized Internet specific configuration. Please refer next section 7.3 to get more details about the Centralized Internet Configuration.
7.3 Centralized Internet Nodes Configuration

First deploy Accelerator nodes at all the sites and make sure they are online by following the steps mentioned in Chapter 3.

Once all the nodes of Centralized Internet Sites are UP then configure the unique Private Network Address on each site via BlueJeans Admin Portal.

7.3.1 Configuration concepts with example

Let’s take an example to understand this process. Below is one Centralized internet setup with two sub sites and one Main Site which is connected to internet.

* Public IP & Private Network Address mentioned above is just for reference.
* Attendees in these sites are associated with anyone of the Private Network Addresses mentioned in that site.
Each Accelerator node is configured with unique Private Network Address from where attendees will join Primetime event.

Example of configuration on each Accelerator nodes:

- Accelerator 1– 10.10.0.0/16, 192.168.10.0/24
- Accelerator 2– 10.20.0.0/16, 192.168.20.0/24
- Accelerator 3 – 10.30.0.0/16, 192.168.30.0/24

7.3.2 Configure Private Network Address via Admin Portal

The steps below will help you to configure Private Network addresses on Accelerator nodes deployed in centralized internet configuration.

- Login to your BlueJeans account by using your Enterprise Username & Password at URL: https://bluejeans.com
- Once you access your account then navigate to Admin -> Manage Accelerator.
- All the nodes deployed in an enterprise are displayed here.
- Click on Edit icon of a node which is the part of centralized internet setup.
- Here add Private Network Addresses under Centralized Internet section and use space bar, enter key or comma “,” button to enter the configuration.
* This example shows the Private Network Address configuration on SiteA.

- Click on “SAVE” button after adding Private Network Addresses to save the configuration.

---

**Note:** Deploy Accelerator nodes in all the sites of Centralized Internet setup. Make sure that attendees from all the sites should be able to reach all the deployed nodes.

For example in Centralized Internet Setup mentioned in last section, attendees of SiteA should be able to access Accelerator nodes of Main Site and SiteB. Similarly, attendees of Main Site should be able to access Accelerator nodes of SiteA and SiteB. This is mandatory requirement in order to select the correct Accelerator Node for attendees to stream Event.
8 HTML5 support on Accelerator

- Introduction
- Prerequisites
- Certificate Provisioning
- Steps for configuring New Accelerator for HTML5 support
- Simplified Provisioning

8.1 Introduction

Accelerator support HTML5 players to stream via it. For Flash player no extra configuration on Accelerator is required but to support HTML5 admin has to do additional configuration on Accelerator.

HTML5 player uses HTTPS to stream via Accelerator. For SSL/TLS communication between server (Accelerator) and client (Attendee), we have to include Certificate & Private key in .pem format (without passphrase) on Accelerator. This chapter is a setup guide for HTML5 Accelerator.

---

NOTE:

- Please contact BlueJeans Customer Support in order to enable HTML5 on Accelerator after importing certificates and Private keys on Accelerator nodes.
- In order to opt-in for simplified provisioning, jump to section 8.5. And you can skip the whole manual process of certificate provisioning.

---

8.2 Prerequisites

- Latest OVF / Accelerator Software: BlueJeans_Accelerator_V2.6
- SSL Certificate and Private Key for each Accelerator node.
- Fully managed internal PKI for Enterprise (recommended)

---

NOTE:

- While generating SSL certificate for an Accelerator set Subject Alternative Name (SAN) under DNS and IP to its Private IP address. In case of multiple nodes (for convenience sake), you can enter up to 11 Private IPs as SAN under a single certificate. Some common FAQs related to accelerator can be found here.
o Firefox browser does not use system trust store; therefore, enterprise root CA should be manually imported into browser Trust store.
  o Please check [here](#) for HTML5 player supported browsers.

### 8.3 Certificate Provisioning

1. Create certificate signing request [with CN (suitable FQDN) and subject alternative name (SAN) with Private IP] of each Accelerator Node.

2. Get this CSR signed by internal enterprise Root CA.

---

**Note:**
- Make sure the signed certificate and the private key is generated in .pem file format (base64 encoded) and should not have passphrase, as this is the only format accepted while importing the certificate and private key onto the Accelerator.
- If there is no enterprise Root CA available, then self-signed certificates can be created using OpenSSL and imported on the Accelerator node. Refer to [Annexure 1](#) for instructions to generate self-signed certificate

---

3. Install signed certificate on Accelerator Node. (Please refer next section 8.4 for more details)

4. Push the enterprise root CA to all streaming endpoints (user systems like desktops/laptops which will receive Primetime Event stream via Accelerator).
Note: Make sure the signed certificate and the private key is generated in .pem file format (base64 encoded) and should not have passphrase, as this is the only format accepted while importing the certificate and private key onto the Accelerator.

8.4 Steps for configuring Accelerator for HTML5 support

This section will help admin to import Certificate & Private Key on Accelerator.

Steps:
1. Deploy Accelerator Nodes. (Please refer Admin Guide Chapter3)

2. After deployment, SSH to Accelerator node, you will find Main Menu.
3. Here select option “[4] SSL Settings”. This will show Sub Menu with following three options:
   [1] View/Edit Signed certificate
   [2] View/Edit private key
   [3] To go to main menu

4. Here select option “[1] View/Edit Signed certificate”. This will show Certificate on this Node. Initially no certificate is imported therefore select “y” to import certificate. Here copy paste certificate (should be .pem file format) and press Enter (twice).
5. Now again select option “[4] SSL Settings” in Main menu and further select option “[2] View/Edi0074 private key” in Sub-Menu. This will show Private Key on this Node. Initially no key is imported therefore select “y” to import Private Key. Here Copy paste Private Key (should be .pem file format without passphrase) and press Enter (twice).
6. Now select Option “[8] Reboot” on Main menu to reboot Accelerator and then select “y” to reboot Accelerator, in order to apply above certificate and Private Key.
7. After reboot, attendees can stream Accelerator node using HTML5 player.

---

**Note:**

- Make sure all the Attendees should have Enterprise Root CA (from which Certificate is issued to Accelerator Node) on their system before streaming Primetime Event via Accelerator node using HTML5 Player.
- Firefox browser does not use system trust store, therefore Enterprise root CA should be manually imported into browser trust store.
8.5 Simplified Certificate Provisioning

Once the feature for simplified provisioning is enabled and an Accelerator node is booted, BlueJeans Cloud Service generates a CA authorized certificate, manages its lifecycle for you and takes care of the renewal process.

---

NOTE: Please contact BlueJeans Customer Support in order to enable Simplified Provisioning for Accelerator nodes.

---

8.5.1 Benefits of Simplified Provisioning

Enterprise Admins do not need to maintain a fully managed PKI anymore. It eliminates the efforts of generating the self-signed certificate and key, copying them to the Accelerator Node and also expels the worrying about expiration of it. As this will not be a self-signed certificate, Attendees won’t be asked to accept the certificate to proceed further.

---

NOTE: Please make sure that you have Latest OVF (Accelerator Software: BlueJeans_Accelerator_V2.9 or above).

---
9 Annexures

- Annexures 1: Generate Self-signed Certificate

9.1 Annexure 1: Generate self-signed certificate

This section will help you to generate self-signed certificate and private key for Accelerator.

Self-signed certificates that will be installed on Accelerator nodes, can generated using BlueJeans scripts which can be downloaded from here.

Prerequisite: Linux server with latest version of openSSL installed.

9.1.1 Steps to Generate Certificate

Please refer below steps to generate certificate and private key of Accelerator:

1. Download file `<cert_scripts.tar.gz>` from here on linux machine.

2. Untar the downloaded file using cli command: `tar -xvf cert_scripts.tar.gz`

3. Go to the folder “cert_scripts” using cli command: `cd cert_scripts/`

4. Generate Root CA:
   a. Using vi editor, modify file “rootCA.cnf” and change following entries:
      • countryName
      • stateOrProvinceName
      • localityName
      • 0.organizationName
      • organizationalUnitName
      • commonName
      • emailAddress

      (Note: Currently default settings are according to BlueJeans)

   b. Give execute permission to the file “createRootCA.sh” and execute it using following cli commands:
      • `chmod +x createRootCA.sh`
      • `./createRootCA.sh`
c. During execution of file, follow onscreen instructions. Here, you will be asked for passphrase. Please provide a strong passphrase. (Note: Remember it for later use as mention in section 6.c).

d. This execution will generate two files:
   i. rootCA.key: needs to kept secretly(never compromised)
   ii. rootCA.pem: must be distributed internally to all streaming endpoints (user systems like desktops/laptops which will receive Primetime Event stream via Accelerator)

5. Generate Accelerator certificate:
   a. Using vi editor, modify file “server.csr.cnf” and change following entries:
      i. countryName
      ii. stateOrProvinceName
      iii. localityName
      iv. organizationName
      v. organizationalUnitName
      vi. commonName (Note: Do not edit it.)
      vii. emailAddress
   (Note: Currently default settings are according to BlueJeans.)

   b. Give execute permission to the file “createselfsignedcertificate.sh” and execute it using following cli commands:
      i. chmod +x ./createselfsignedcertificate.sh
      ii. ./createselfsignedcertificate.sh <Accelerator IP>
   (Example: ./createselfsignedcertificate.sh 192.168.1.10)
   (Note: It’s must to use only Accelerator Private IP here.)

   c. During execution of file, follow onscreen instructions. When asked for passphrase for rootCA, enter the passphrase that was entered previously (in above step 4.c).

   d. This execution will generate two files:
      i. server_<IP>.crt (certificate)
      ii. server_<IP>.key (private key)

Once you generate Certificate and Private Key for Accelerator, then import them on respective Accelerators. Please refer Chapter 8.4.