# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change History</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Installation</td>
<td>5</td>
</tr>
<tr>
<td>Product compatibility</td>
<td>5</td>
</tr>
<tr>
<td>Minimum Load Line-up Dependencies</td>
<td>5</td>
</tr>
<tr>
<td>Product Release Matrix</td>
<td>5</td>
</tr>
<tr>
<td>What’s New</td>
<td>6</td>
</tr>
<tr>
<td>Avaya Aura® Web Gateway</td>
<td>6</td>
</tr>
<tr>
<td>New in the 3.2 release:</td>
<td>6</td>
</tr>
<tr>
<td>Unified Portal</td>
<td>6</td>
</tr>
<tr>
<td>New in the 3.2 release:</td>
<td>6</td>
</tr>
<tr>
<td>Managing Equinox Clients on Portal:</td>
<td>7</td>
</tr>
<tr>
<td>Limitations &amp; Restrictions</td>
<td>9</td>
</tr>
<tr>
<td>Fixes</td>
<td>10</td>
</tr>
<tr>
<td>Release 3.2</td>
<td>10</td>
</tr>
<tr>
<td>Avaya Aura® Web Gateway</td>
<td>10</td>
</tr>
<tr>
<td>Known issues and workarounds</td>
<td>14</td>
</tr>
<tr>
<td>Release 3.2</td>
<td>14</td>
</tr>
<tr>
<td>Avaya Aura® Web Gateway</td>
<td>14</td>
</tr>
<tr>
<td>Unified Portal</td>
<td>15</td>
</tr>
<tr>
<td>Documentation</td>
<td>17</td>
</tr>
<tr>
<td>Documentation Errata</td>
<td>17</td>
</tr>
</tbody>
</table>
Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/10/2017</td>
<td>July GA update for Avaya Aura® Web Gateway 3.2.</td>
</tr>
</tbody>
</table>

Introduction

This document provides information to supplement the Avaya Aura Web Gateway and the Unified Portal Release 3.2 (used in Equinox Conferencing Release 9.0.2) GA software and documentation. For updated documentation, product support notices, and service pack information, go to the Avaya Support site at http://support.avaya.com.

Please refer to the latest Avaya Aura® 7.1 Release Notes for information specific to the Avaya Aura® feature and service packs.
Installation

Product compatibility

For the latest and most accurate compatibility information go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Minimum Load Line-up Dependencies

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avaya Aura® System Manager</strong></td>
<td>7.1.0.0 Build 1125193 Software Update Revision No: 7.1.0.0 Build 116662</td>
</tr>
<tr>
<td><strong>Avaya Aura® Session Manager</strong></td>
<td>7.1.0.0 Build 710028</td>
</tr>
<tr>
<td><strong>Avaya Aura® Presence Services</strong></td>
<td>7.1.0.0 Build 600</td>
</tr>
<tr>
<td><strong>Avaya Equinox Conferencing</strong></td>
<td>9.0.2</td>
</tr>
</tbody>
</table>

Product Release Matrix

The following table lists the release build numbers of the Avaya Equinox clients and required infrastructure servers.

<table>
<thead>
<tr>
<th>Client/Server</th>
<th>Release Build Number</th>
<th>Date Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Equinox for Windows</td>
<td>3.2.0.33</td>
<td>10 July 2017</td>
</tr>
<tr>
<td>Avaya Equinox for MacOS</td>
<td>3.2.0.16</td>
<td>10 July 2017</td>
</tr>
<tr>
<td>Avaya Equinox for Android</td>
<td>3.2.0.54</td>
<td>10 July 2017</td>
</tr>
<tr>
<td>Avaya Equinox for iOS</td>
<td>3.2.0.43</td>
<td>10 July 2017</td>
</tr>
<tr>
<td>Avaya Multimedia Messaging</td>
<td>3.2.0.0 Build 372</td>
<td>10 July 2017</td>
</tr>
<tr>
<td>Avaya Aura® Device Services</td>
<td>7.1.0.0 Build 363</td>
<td>10 July 2017</td>
</tr>
<tr>
<td>Avaya Aura® Web Gateway</td>
<td>3.2.0.0 Build 412</td>
<td>10 July 2017</td>
</tr>
</tbody>
</table>
What's New

Avaya Aura® Web Gateway

The Avaya Aura® Web Gateway is an Aura server acting as a gateway to Aura for clients and applications utilizing browser based WebRTC signaling and media.

In Team Engagement Aura deployments, the components of this gateway (Endpoint Service Gateway and Web Portal) are provided on a Single OVA for deployment in a Customer supplied VMware environment. These components are shared and utilized by different Aura clients and Applications.

In Over the Top non-Aura Equinox™ Conferencing deployments, these components are hosted within the Equinox Conferencing solution.

New in the 3.2 release:

The following services are new when using AAWG with Avaya Equinox 3.2 Clients:

- **Scopia Desktop Client Replacement, new deployment mode**
  - HTTP Conferencing (SIP not required)
    - Guest conference users
    - Signed in Equinox Conferencing users
    - Mid-conference controls
    - Integration into Top of Mind and Click to Join
  - Unified Portal integration
  - Launch from Unified Portal
  - Discovery of personal virtual rooms
  - Enhanced conference call logs
  - Presentation only mode (no audio and no video call)
  - In-conference branding for calls

Unified Portal

The Unified Portal web client is the new WebRTC based meet-me client for the Scopia solution 8.5. It replaces the existing Scopia Desktop user portal and the Scopia Management user portal clients, while adding new capabilities.

New in the 3.2 release:

- Scopia Desktop Client Replacement feature allows the use of Equinox Clients products similar to the Scopia Desktop Client (SDC) in the previous release.
- Picture Service allows users and administrators to set up avatars for signed-in users via LDAP or Portal settings.
- A lot of UX improvements to make the user experience better.
Managing Equinox Clients on Portal:

Perform the steps outlined below for Unified Portal to offer the new Equinox clients to users.

NOTE:

a. The following procedure is a replacement for that provided in the Deploying Avaya Aura Web Gateway document – Ch. 6 Administration > Managing clients

b. For a multi-tenant system, the following procedure will have to be repeated for each tenant

To offer fresh equinox client installs for Guest users (in all deployments):

1. Create a zip archive which contains the WindowsOS and MacOS Equinox client installers along with a sparkle.xml file.
   Following is a sample content of the sparkle.xml file to be included in the archive (a similar template is also available on the deployed system at /opt/Avaya/CallSignallingAgent/branding/portal/customstyles/sparkle.xml) –

NOTE:

a. **DO NOT** create additional directories inside the zip archive. Place the installer artifacts and sparkle.xml at the root of the archive (as shown in the sample screenshot below)

b. For MacOS, the fresh install installer must be used, i.e. the .dmg installer file with the word “Sparkle-Update” **not** in the file name

c. When creating the sparkle.xml file, make sure to replace the text in red below with the appropriate equinox client installer version numbers

d. For a multi-tenant system, the sparkle.xml URLs in each tenant-specific zip archive must contain the respective tenant alias, instead of ‘999’
   For example, 999 in enclosure url should be changed to your tenant alias:
   <enclosure url="/portal/custom-styles/999myTenantAlias/Avaya Equinox 3.2.0.14.dmg"
2. On the Equinox (iView) Management UI, navigate to Settings tab > Branding menu item. Upload the archive created in Step 1. above to the "User Portal Server" section and hit Apply.

**NOTE:**

a. **Before uploading**, if you had previously uploaded branding files for User Portal, you **must** first go back and add those branding files to the new archive in Step 1. above

Repeat the above procedure in order to update the Equinox client installers to be offered to Guest Users for fresh client installs (i.e. new zip archive(s) containing the installers and updated version numbers in the sparkle.xml).

**To offer equinox client upgrades for all users:**

**NOTE:** For MacOS, the update installer must be used, i.e. the .dmg installer file with the word “Sparkle-Update” in the file name.

For Equinox OTT (non-Aura) Deployments:

1. On the Equinox (iView) Management UI, navigate to Settings tab > User Portal / Web Gateway menu item > Equinox Client
2. Click "Upload the client", set version, title and file to upload. Repeat for both Mac and windows clients.

For Equinox Team Engagement (TE+Conf) Deployments:

1. On the AADS Admin UI, navigate to Settings tab > User Portal / Web Gateway menu item > Equinox Client
2. Click "Upload the client", set version, title and file to upload. Repeat for both Mac and windows clients.

**Limitations & Restrictions**

<table>
<thead>
<tr>
<th>#</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Minimum Chrome browser version for WebRTC calls needs to be 53 or above</td>
</tr>
<tr>
<td></td>
<td>If auto update doesn’t work, the user may have to explicitly download and install the newer version of Chrome to get to version 53 or above</td>
</tr>
<tr>
<td>2</td>
<td>AAWG and Scopia use two different methods to show the relative offset from GMT. One format tells you how far behind UTC you are (Thu Nov 3 13:47:41 GMT-7 2016), while the other tells you how many hours to add to be the same as UTC (Thu Nov 3 12:51:59 GMT+6 2016).</td>
</tr>
</tbody>
</table>
## Fixes

The following tables are cumulative since the last minor release showing the most recent release first and oldest release.

### Release 3.2

**Avaya Aura® Web Gateway**

<table>
<thead>
<tr>
<th>ID</th>
<th>Summary</th>
<th>Found in Release</th>
<th>Resolved in Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVERCSDK-2834</td>
<td>Sometimes input fields are unavailable in Admin GUI in Internet Explorer (IE).</td>
<td>3.0.0.0</td>
<td>3.2</td>
</tr>
<tr>
<td></td>
<td><strong>Workaround:</strong> Refresh page</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SERVERCSDK-4217</td>
<td>STUN priority page isn't updated when all STUN servers are deleted. Old and duplicated entries could be in the STUN priority list.</td>
<td>3.1</td>
<td>3.2</td>
</tr>
</tbody>
</table>
|               | **Workaround:**  
|               |   - Add a fake STUN server  
|               |   - Add STUN servers you want to remove from the priority list  
|               |   - Delete servers added in the step 2. Now you should have only fake STUN server in list  
|               |   - Add STUN servers you are going to use.  
|               |   - Delete the fake STUN                                               |                  |                     |
| SERVERCSDK-4218 | AAMS priority can contain stale entries if location is removed or renamed in SMGR. New location names are not in AAMS priority list. | 3.1              | 3.2                 |
|               | **Workaround:**  
|               |   - Remove old location from AAMS priority  
|               |   - Add new location name to AAMS priority list, it is available in excluded location list  |                  |                     |
| SERVERCSDK-4224 | Location priority section isn’t updated when location is chosen for AAWG node; STUN priority list is not updated when STUN server added to the list | 3.1              | 3.2                 |
|               | **Workaround:** Refresh browser page                                   |                  |                     |
Remote Web MeetMe encounter 502 Bad Gateway after upgrade to 3.1

Workaround:
Ssh into aawg
Edit remote-access-port.conf

```
sudo vi
/opt/Avaya/CallSignallingAgent/3.1.0.0.622
/nginx/1.8.0-1/conf/remote-access-port.conf
```

Delete existing contents of the file and replace with the following

**NOTE:** Make sure you replace the content within !!!...!!! below (with your node fqdn & your remote port)

```
server {
    error_log
    /opt/Avaya/CallSignallingAgent/3.1.0.0.622
    /logs/nginx/1b_error.log warn;
    access_log
    /opt/Avaya/CallSignallingAgent/3.1.0.0.622
    /logs/nginx/1b_access.log;
    access_log
    /opt/Avaya/CallSignallingAgent/3.1.0.0.622
    /logs/nginx/1b_security.log security_log
    if=$rest_client_security_log;

    ssl_certificate
    /opt/Avaya/CallSignallingAgent/3.1.0.0.622
    /CAS/3.1.0.0.622/nginx/certs/nginx.crt;
    ssl_certificate_key
    /opt/Avaya/CallSignallingAgent/3.1.0.0.622
    /CAS/3.1.0.0.622/nginx/certs/nginx.key;

    server_name !!!node-fqdn!!!;

    add_header X-Load-Balancer
    !!!node-fqdn!!!;

    include secure-headers.conf;
    include
    enable_ssl_verify_client_rest.conf;
    #include no-cache.conf;
    add_header Pragma no-cache always;
    add_header Cache-Control no-cache,must-revalidate,private always;

    proxy_set_header Host
    $host:$server_port;
    proxy_set_header X-Forwarded-For
    $proxy_add_x_forwarded_for;

    # Clear Connection header to enable keep-alive
```
proxy_set_header Connection "";

# ESG doesn't have client context
on the over nodes and if we fail over
request to another node we get 404 not
found

# Removed failing over for 500,
502, 504 errors
proxy_next_upstream error
timeout;

listen !!!remote_port!!!;

limit_req zone=rest burst=50
no_delay;

# Give enough read timeout for
long polls; we'll rely on downstream nginx
to handle connect timeouts to the backend
web container.
proxy_read_timeout 800;
proxy_connect_timeout 800;

ssl_client_certificate
/opt/Avaya/CallSignallingAgent/3.1.0.0.622
/CAS/3.1.0.0.622/nginx/certs/auth_ca.crt;

set $certificate_validation_failure false;
if ($ssl_client_verify !=
"SUCCESS") {
  set $certificate_validation_failure true;
}  
set $validation_flag
"${enable_ssl_verify_client_rest}_${certificate_validation_failure}";
if ($validation_flag =
"on_true"){
  return 400;
}

set_escape_uri
$ssl_client_cert_for_tomcat
$ssl_client_raw_cert;

location / {
  proxy_set_header Upgrade
$http_upgrade;
  proxy_read_timeout 800;
  proxy_connect_timeout 800;
  proxy_set_header Connection
$http_connection;
  proxy_set_header X-Avaya-
  External-Request " ";
limit_req zone=rest burst=50 nodelay;
error_page 500 502 504 @fallback;
proxy_pass https://amm_servers_
sticky;
proxy_ssl_certificate /opt/Avaya/CallSignallingAgent/3.1.0.0.622/CAS/3.1.0.0.622/nginx/certs/nginx-s2s.crt;
proxy_ssl_certificate_key /opt/Avaya/CallSignallingAgent/3.1.0.0.622/CAS/3.1.0.0.622/nginx/certs/nginx-s2s.key;

# Adding header for server-to-
server authentication.
# Also is should wipe the
header data if provided by client
proxy_set_header X-SSL-Client-S-DN $ssl_client_s_dn;
proxy_set_header X-Client-Cert $ssl_client_cert_for_tomcat;
proxy_set_header REQUEST-ORIGIN REST;
include cors-service.conf;
}

# Requests to the Multi-Site
resource are blocked.
location /aem/resources/site {
  return 404;
}

# The sticky module doesn't honor
proxy_next_upstream. However, should
# we get an error, we'll fallback
to this set of servers, which are
# not sticky. This causes a
different server to be used (respecting
# proxy_next_upstream), a new
cookie to be set, and a new server to
# become the session owner.
location @fallback {
  proxy_set_header Upgrade $http_upgrade;
  proxy_set_header Connection $http_connection;
  proxy_set_header X-Avaya-External-Request " ";
  proxy_pass https://amm_servers_
}
## Known issues and workarounds

### Release 3.2

**Avaya Aura® Web Gateway**

<table>
<thead>
<tr>
<th>ID</th>
<th>Summary</th>
<th>Found in Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVERCSDK-3459</td>
<td>ESG Cores displays UTC time Instead of displaying configured NTP time GMT.</td>
<td>3.0.0.0</td>
</tr>
<tr>
<td>SERVERCSDK-3623</td>
<td>No audio from ACW to AAWG client after video escalate</td>
<td>3.0.0.0</td>
</tr>
<tr>
<td></td>
<td><strong>Workaround:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Go to Media Settings -&gt; Audio in admin UI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remove G726 coded from SIP audio codecs list</td>
<td></td>
</tr>
<tr>
<td>SERVERCSDK-4297</td>
<td>Video is negotiated to &quot;sendrecv&quot;, but no video is displayed.</td>
<td>3.1</td>
</tr>
<tr>
<td></td>
<td><strong>Workaround:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Need to set the Direct IP-IP Audio Connections setting to &quot;y' on CM.</td>
<td></td>
</tr>
<tr>
<td>SERVERCSDK-4246</td>
<td>After fresh install, certificate needs to be re-applied to AAWG/Portal from iView.</td>
<td>3.2</td>
</tr>
<tr>
<td>SERVERCSDK-4576</td>
<td>Back to back mid-call operations (i.e. add/remove video, hold/unhold calls) are resulting in no video when being performed using Chrome browser version 58.0.3029.81.</td>
<td>3.2</td>
</tr>
<tr>
<td></td>
<td>This issue is only seen with MCU 7K calls.</td>
<td></td>
</tr>
<tr>
<td>SERVERCSDK-4675</td>
<td>With the Equinox Conferencing 9.0.2 solution, end users will receive the following message when the conference has reached the maximum number of participants.</td>
<td>3.2</td>
</tr>
<tr>
<td></td>
<td>&quot;Sorry, cannot join the specified meeting. Please contact the system administrator.&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Before contacting an administrator, please check the number of participants in the conference and if it is less than the maximum allowed, please contact the administrator.</td>
<td></td>
</tr>
<tr>
<td>SERVERCSDK-4699</td>
<td>Due to an issue with Chrome browser handling of self-signed certificates, the following step is needed when accessing AAWG Administrator UI with Chrome Browser:</td>
<td>3.2</td>
</tr>
<tr>
<td></td>
<td>Clear the browser cache and restart the Chrome browser before accessing the administrator UI.</td>
<td></td>
</tr>
</tbody>
</table>
### Unified Portal

<table>
<thead>
<tr>
<th>#</th>
<th>Component</th>
<th>Description</th>
<th>Workaround\fix</th>
</tr>
</thead>
</table>
| 1  | Authentication| Cannot login to Portal via IE for Team Engagement and Conference deployments using Internet Explorer 11. | Login to AADS admin console, open Client Administration -> Client Settings and select NONE in REST field. | Setup checklist:  
  (AADS) set the REST cert policy to NONE – this is related to 8443 port.  
  (AADS) apply the new dynamicconfig patch to open 8440.  
  (AADS) CORS should be enabled since Portal hosted to other domain.  
  (AAWG/Portal) set Server-To-Server port as 8440, set Client port as 8443. After this AAWG will work over 8440, Portal will work over 8443 like early.  
  (AAWG) NONE is default in latest loads. |
| 2  | Scopia Mobile | Meeting via Unified Portal on Safari - iOS device cannot join any meetings   | Reload Portal page |

<table>
<thead>
<tr>
<th></th>
<th>3  Scheduling</th>
<th>It's not possible to change single meeting to series and vice versa</th>
<th>UPC-1522 - It is not possible to add recurrence to the existing meeting in future. Closed When edit existing meeting make recurrent button will be disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4  Mobile:Android</td>
<td>Cannot copy link for Androids 5+ as execCommand doesn't support more. For now this should be implemented via Chrome Extensions. Will be proposed as enhancement for next release.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5  Mobile:Safari</td>
<td>Copy link doesn't work on Safari 9.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6  Chrome:Broadcast</td>
<td>To watch a broadcast via Chrome browser Flash player should be installed</td>
<td>Intend behavior for 3.2</td>
</tr>
<tr>
<td></td>
<td>7  EC: Presentation</td>
<td>Callback parameter won't be passed correctly even if it's provided during join via Portal</td>
<td>Rare case for end-user</td>
</tr>
</tbody>
</table>
Documentation

For Avaya Aura® Web Gateway 3.2, the following documents have been updated on the support site:

<table>
<thead>
<tr>
<th>Guide</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying the Avaya Aura® Web Gateway</td>
<td><a href="https://downloads.avaya.com/css/P8/documents/101041361">https://downloads.avaya.com/css/P8/documents/101041361</a></td>
</tr>
</tbody>
</table>

Documentation Errata

None.
Contacting support

Contact Support Checklist

If you are having trouble with the Avaya Aura® Web Gateway, you should:

1. Set log level to debug.
2. Retry the action. Carefully follow the instructions in written or online documentation.
3. Check the documentation that came with your hardware for maintenance or hardware-related problems.
4. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.

If you continue to have a problem, contact Avaya Technical Support:

2. Contact Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Web site.

Contact Support Tasks

You may be asked to email one or more files to Technical Support for analysis of your application and its environment.