Security

User administration and authentication

MediaSense supports three types of users: API users, application administrators, and platform administrators. There is only one application administrator and one platform administrator. Both of these users are configured during installation and the credentials for them are stored on MediaSense. Any number of API users can be configured after the installation process is complete.

For API users, MediaSense uses Unified Communications Manager's user administration. Any users configured as end users in Unified Communications Manager may be enabled as MediaSense API users. Once signed in to MediaSense, any such user can access all API functions. API clients sign in using a MediaSense API request, but MediaSense delegates the actual authentication of the user to Unified Communications Manager using the AXL service. API user passwords are maintained in Unified Communications Manager only and are not copied to MediaSense.

MediaSense does not currently support the notion of multiple roles and authorizations.

MediaSense APIs and Events

MediaSense API interactions are conducted entirely over secure HTTPS. All API requests must be issued within an authenticated session, denoted through a JSESSIONID header parameter. Authentication is accomplished through a special sign-in API request. However, SWS events are only delivered to clients using HTTP; HTTPS is not currently supported for eventing. By default, MediaSense uses self-signed certificates, but customers may install their own. When certificates are provided by clients, MediaSense always accepts them and does not verify their authenticity.

Internal intracluster communication

Components in a MediaSense cluster communicate with each other over unencrypted HTTP or Java Messaging Service (JMS) connections. The specifications for these interactions are not publicly documented, but they cannot be considered to be secure.

Media output URIs

A number of HTTP, HTTPS, and RTSP URIs may be associated with each recorded session. HTTPS URIs are secure by definition, but their security extends only to the transport mechanism. The URIs themselves can be transmitted insecurely by people or equipment.

To prevent unauthorized users from making inappropriate use of these media output URIs, MediaSense requires that HTTP-BASIC authentication credentials be provided every time such a URI is used. In other words, a client must authenticate itself as a valid API user before it is given access to the recorded media. This authentication is usually very fast, but it may occasionally take up to 4 seconds to complete.

Uploaded media files

Administrator credentials are required to upload videos for ViQ, VoH and VoD purposes. The administration interface includes links that can be used to download previously uploaded MP4 files. Although administrator credentials are required to access the interface, the download links do not require credentials, and therefore cannot be considered as secure.

Media

Media encryption in transit, using Secure RTP (sRTP) or other means, is currently not supported. Media may however be stored on an encrypted SAN, as long as disk throughput requirements are met. Provisioning and configuring SAN encryption is outside the scope of MediaSense information.