# Ports and Network Configuration Requirements

September 2018

Part Number: 551-00077-00 Rev 11

## Overview

**Affected Products/Components:** Prysm Application Appliances running Prysm Release 2.x and later

This bulletin describes the network ports and configuration requirements for a Prysm Application Appliance deployed against either the Prysm Hosted Cloud or a Customer Hosted Cloud server (On-Premise VM).For details, see:

- Prysm Hosted Cloud (PHC)
- Customer Hosted Cloud (CHC)

> **Note:** Additional network ports required for optional features fall outside the scope of this bulletin: Interactive Input Controllers, Remote Desktop Protocol (RDP) - TCP 3389, Active Directory (LDAP) - TCP 389, Skype for Business Protocols - TCP/STUN 443, VTC Codec and Socket API integration with 3rd Party Automation Controllers.

## Assumptions and Prerequisites

- The ports listed represent the factory configuration for each scenario.
- No inbound firewall rules are required. All network communication originates from the Prysm Application Appliance.
- Customer's network environment must support typical HTTP and HTTPS web traffic via ports 80 and 443.
- Prysm for rooms, Prysm for web, and Admin Portal initiated API communication to the Prysm Hosted Cloud or Customer Hosted Cloud that target port 80 are immediately redirected and enforce secure HTTPS via port 443.

# Prysm Hosted Cloud

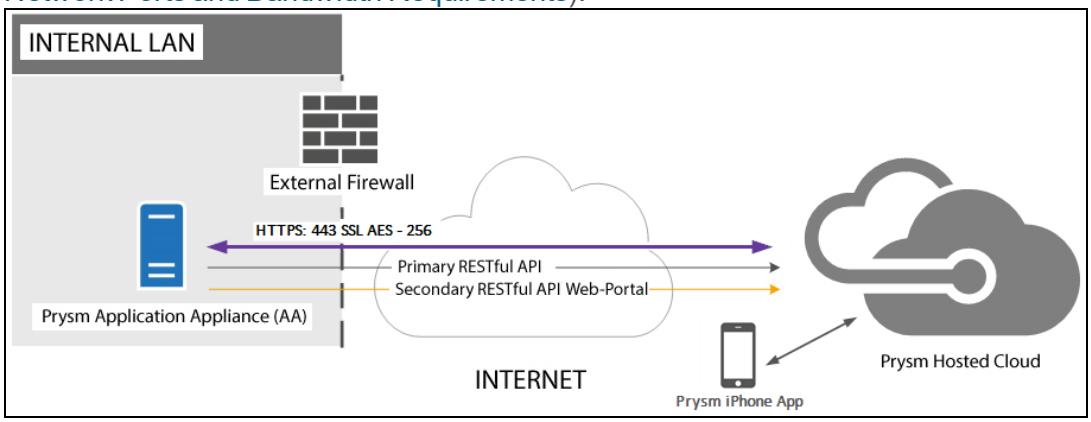
> **Note:** This section applies only to the Prysm Hosted Cloud. For information on a Customer Hosted Cloud Server, see "Customer Hosted Cloud Server" on page 7.

## Network Ports and Requirements

Prysm leverages a modern client-server software architecture where the client is an end-user facing software application that runs on a Prysm Application Appliance. The server, referred to as the Prysm Hosted Cloud, is a multi-tenant platform-as-a-service (PAAS) comprised of a stack of microservices running behind an API gateway. The Prysm Hosted Cloud uses Microsoft Azure to provide a high security, high reliability, scalable and low latency infrastructure.

The IP-based communication between Prysm Application Appliance and the Cloud leverages a RESTful API. This API enforces strict HTTPS to ensure that all traffic is signed and encrypted. This includes all device configuration, user authentication, file transfer and meta-data synchronization with the Prysm instance(s) deployed in each customer's environment. In addition, Prysm Admin Portal, a Web-based management portal, also strictly enforces HTTPS and is built on the same RESTful API. Prysm Admin Portal provides the means for a credentialed administrator to configure the settings and features available to users as well as create and manage users, groups and permissions. In addition to HTTPS enforcement, all file-based customer content is encrypted using symmetric AES 256 with a minimum 1024-bit key encryption at the time of upload and remains encrypted ‘at-rest’ within the Prysm Hosted Cloud.

The minimum bandwidth requirement for communication between the Prysm Application Appliance and the Prysm Hosted Cloud is 1.5 Mb/s, and Prysm recommends at least 3 Mb/s. This minimum requirement supports using a Prysm-enabled display only for project files, annotation, whiteboarding, sticky notes and text. Additional bandwidth is required for device sharing and co-browsing (see Device Sharing and Co-browsing Network Ports and Bandwidth Requirements).

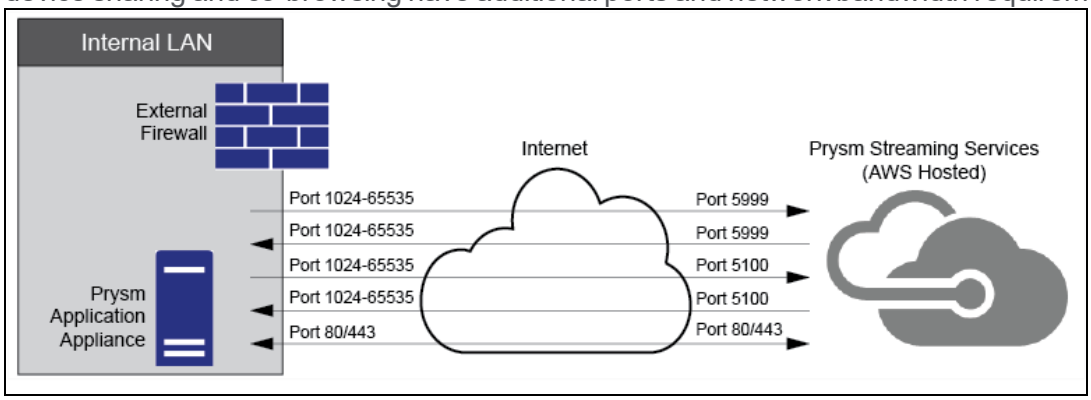


| Port | Protocol | Source | Destination | Direction | Network Interface | Description |
|---|---|---|---|---|---|---|
| 80/443 | HTTP/ HTTPS | <IP Address of Prysm AA> | admin.prysm.com | Unidirectional | Internet/ (Unsecured-WAN circuit) | Access to Prysm Admin Portal for user and device administration. |
| 80/443 | HTTP/ HTTPS | <IP Address of Prysm AA> | api.prysm.com | Unidirectional | Internet/ (Unsecured-WAN circuit) | Client Server API through which all authentication, collaboration and file transfer occurs. |
| 80/443 | HTTP/ HTTPS | <IP Address of Prysm AA> | identity-prd.prysm.com | Unidirectional | Internet/ (Unsecured-WAN circuit) | Prysm user authentication URL. |
| 12201 | UDP | <IP Address of Prysm AA> | log.prysm.com | Unidirectional (outbound) | Internet/ (Unsecured-WAN circuit) | For logging purposes.** (Default is Syslog Level 6 - Informational). The list of severities is defined by RFC 3164. |
| 587 | SMTP | <IP Address of Prysm AA> | <IP Address of Organization's Mail Relay Server> | | Internet/ (Unsecured-WAN circuit) | *Optional*. For outbound e-Mail using the Share e-Mail feature. |

**Note:** Prysm services are dynamically assigned IP addresses which are perpetually subject to change within Microsoft Azure.
Customer firewall rules should specify the fully qualified domain name (FQDN) to mitigate the risk of required traffic being blocked as a result of an assigned IP address changing.

## Device Sharing and Co-browsing Network Ports and Bandwidth Requirements

Prysm leverages the Amazon Web Services cloud for Device Sharing and Co-browsing. Deployments with device sharing and co-browsing have additional ports and network bandwidth requirements.




| Source | Source Port | Protocol | Protocol | Destination Port | Direction | Description |
|---|---|---|---|---|---|---|
| <IP Address of Prysm AA> | 1024 - 65535 * | UDP | <Streaming Server> ** | 5999 | Unidirectional (producer) | Outbound stream establishment to cloud-based streaming servers. Supports device sharing between in-room displays and Prysm for web participants. |
| <Streaming Server> ** | 5999 | UDP | <IP Address of Prysm AA> | 1024 - 65535 * | Unidirectional (producer) | Inbound stream establishment response from cloud-based streaming servers. Supports device sharing between in-room displays and Prysm for web participants. |
| <IP Address of Prysm AA> | 1024 - 65535 * | UDP | <Streaming Server> ** | 5100 | Unidirectional (producer) | Outbound media stream to cloud-based streaming servers. Media is protected by DTLS. Supports device sharing between in-room Appliances and Prysm Streaming services. |
| <Streaming Server> ** | 5100 | UDP | <IP Address of Prysm AA> | 1024 - 65535 * | Unidirectional (producer) | Inbound proprietary stream status and DTLS connection status between cloud-based streaming servers and Prysm Appliances. |
| <IP Address of Prysm AA> | 80/443 | HTTP/HTTPS | <Streaming Server> ** | 80/443 | Bidirectional (consumer) | HTTP/HTTPS connection to cloud-based streaming servers which Prysm Appliances and Prysm for web participants use to consume streamed media traffic generated by shared devices and co-browsers. |

**Note:**

*** UDP NAT Transversal:** NAT traversal relies on a prior outbound initiated packet using the same ports. Each negotiated stream leverages a single, randomly selected UDP port, which ensures that ports are dynamic and discrete for every established connection.

**** Streaming Server:** streaming-*cloud.prysm.com (For example, directors.cloud.prysm.com)

Prysm cloud-based streaming servers are currently deployed into 3 different regions each with 2 different availability zones. Prysm may move regions or availability zones based on need or scale. The regions and availability zones include:

- Region/AZ
- Us-east-1/us-east-1a
- Us-east-1/us-east-1b
- EU-west-1/eu-west-1a
- EU-west-1/eu-west-1b

Although there is not a fixed list of names or IP addresses that are used, there is a fixed pattern that is used for the DNS name of each destinations: streaming-<env>-<index>-<availabilityzone>.cloud.prysm.com

Firewall rules implemented by each customer should employ the use of a wild card ( * ) within the following destination DNS syntax: >streaming-*.cloud.prysm.com

### Requirements for Prysm Streaming Servers

For Prysm streaming services (such as Live Source Streaming, co-browsers, sharing your desktop, and sharing an application), a logical server name (such as Domain Name) is a required connection capability. Prysm currently uses Fully Qualified Domain Names (FQDN) to identify its servers' dynamic IP addresses for connecting to Prysm streaming servers via UDP. If a customer's network environment does not support FQDNs, the customer must manually update IP addresses for Prysm streaming servers in the network firewall configuration. If the customer doesn't make these manual firewall changes, Prysm's streaming features will be disrupted.

## Device Sharing and Co-browsing Network Bandwidth Requirements

Device sharing (wired and wireless) and co-browsing require additional network bandwidth. The network internet connection must support the number of sources (live sources and co-browsers) being uploaded and downloaded at one time, and insufficient bandwidth may result in a degraded viewing experience. Each source being uploaded requires 1 Mb/s, and each source being downloaded requires 6 Mb/s. The network bandwidth requirements are calculated as follows:

- Estimated stream upload bandwidth = Number of producers * Number of sources * 1 Mb/s
- Estimated stream download bandwidth = Number of consumers * Number of sources * 6 Mb/s

**Example:** For example, assume your team is collaborating in a conference room with 1 Prysm display.

You're sharing 1 wired device to the project. You are producing this stream.

Upload bandwidth requirement = 1 producer * 1 source * 1 Mb/s = 1 Mb/s

Other teams involved in the collaborative session are sharing 2 wireless devices and 2 co-browsers. You are consuming these streams.
Download bandwidth requirement = 1 consumer * 4 sources * 6 Mb/s = 24 Mb/s

If you increase the number of Prysm displays in your environment to 2, but don't create any additional streams, the production bandwidth requirement is unchanged, but the consumption bandwidth requirement doubles.
Upload bandwidth requirement = 1 producer * 1 source * 1 Mb/s = 1 Mb/s
Download bandwidth requirement = 2 consumers * 4 sources * 6 Mb/s = 48 Mb/s

The bandwidth requirements are based on simultaneous meetings using default settings of 1 Mb/s Bitrate and 10 FPS. Increasing the Streaming Bitrate or FPS settings increases the bandwidth requirements.

## Example Access Control List (ACLs) for Prysm Hosted Cloud solution

```
! – admin.prysm.com
access-list 101 permit tcp host <source ip address> host admin.prysm.com eq 80
access-list 101 permit tcp host <source ip address> host admin.prysm.com eq 443
!- api.prysm.com
access-list 101 permit tcp host <source ip address> host api.prysm.com eq 80
access-list 101 permit tcp host <source ip address> host api.prysm.com eq 443
!- log.synthesize.com
access-list 101 permit udp host <source ip address> host log.prysm.com eq 12201
```

** The syslog messages contain transactions between Prysm Application Appliances and the cloud. The messages do not contain any customer data; just the obfuscated file names which cannot be traced back to the source. Below are some examples of the informational syslog messages.

```
2016-05-05 09:10:17.841 4544517315
DOWNLOAD : File: daa98a58-2313-4063-bc06-72c56792aa8d.png hasn't yet been uploaded to cloud 2016-
05-05 09:10:17.808 04154000248
ERROR : FileSyncDownloadService : Exception occurred while downloading file: 36424ebd-7e78-4a41-
8854-aa9e253b1709.png : System.Net.WebException: The remote server returned an error: (404) Not
Found. at System.Net.WebClient.DownloadFile(Uri address)
```

## Wall Unlock with Prysm iPhone App

Using the Prysm iPhone app, a user can unlock a Prysm-enabled display and open projects or a workspace. The display must have the Wall Unlock setting enabled through Prysm Admin Portal.

The iPhone app requires no additional bandwidth or ports. When the unlock code is entered in the app, the iPhone signals the Prysm Hosted Cloud using SSL. Then the Prysm Hosted Cloud relays the unlock code, using SSL, to unlock the display and permit access to the selected project or workspace. All communication between the iPhone, the Prysm Hosted Cloud, and the Prysm Application Appliance is encrypted using SSL. In addition, the unlock codes are reset each time the Welcome page is displayed, when a user signs out or closes Prysm Go.

### Prysm for desktop

Prysm for desktop is supported on Windows 10 devices and is available from the Microsoft Store. Users can download Prysm for desktop using a Live ID, or companies can make the Prysm app available in their private store (as described here) so that employees can easily get it with their Active Directory credentials.

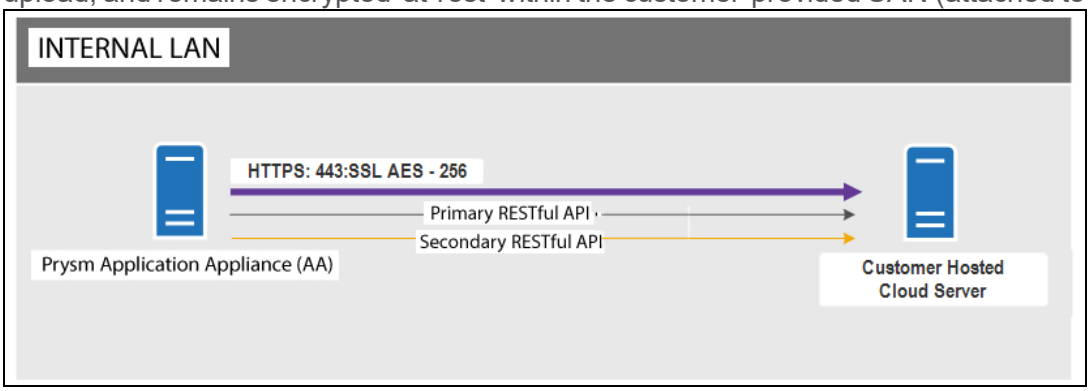
After installing Prysm for desktop, users are prompted to install the Prysm Sharing Agent, which is a supplement to the app that enables local application sharing.

There are no additional port and bandwidth requirements for Prysm for desktop other than those required for all Prysm applications (see here).

## Customer Hosted Cloud Server

> **Note:** This section applies only to the Customer Hosted Cloud. For information on the Prysm Hosted Cloud, see Prysm Hosted Cloud.

The Customer Hosted Cloud deployment option enables customers to host the Prysm Services on a customer provided server which resides entirely behind an organization's firewall. This option enforces HTTPS API communication for all device configuration, user authentication, file, and meta-data synchronization. All file-based content is encrypted using symmetric AES 256 with a minimum 1024-bit key encryption at the time of upload, and remains encrypted 'at-rest' within the customer-provided SAN (attached to the host VM).



| Port | Protocol | Source | Destination | Direction | Network Interface | Description |
|---|---|---|---|---|---|---|
| 4433 | HTTPS | <IP Address of Prysm AA> | <IP Address of VM> | Unidirectional | LAN | Access to Prysm Admin Portal for administration purposes. |
| 80/443 | HTTP/HTTPS | <IP Address of Prysm AA> | <IP Address of VM> | Unidirectional | LAN | Client Server API through which all authentication, collaboration and file transfer occurs. |
| 443 | HTTPS | <IP Address of Prysm AA> | Prysm license entitlement service | Bidirectional | Internet/ (Unsecured-WAN circuit) | Communication between the Customer Hosted Cloud and the Prysm license entitlement service. An internet connection is required for Customer Hosted Cloud servers to communicate with the Prysm license entitlement service to verify and update entitlements for features or user licenses. |
| 587 | SMTP | <IP Address of Prysm AA> | <IP Address of Organization's Mail Relay Server> | Unidirectional | LAN | *Optional*. For outbound e-mail using the Share e-mail feature. |
| 5757 | UDP | <IP Address of Prysm AA> | <IP Address of VM> | Unidirectional | LAN | *Optional*. System health and diagnostics logging. |

## Example Access Control List (ACLs) for Customer-Hosted Cloud Server solution

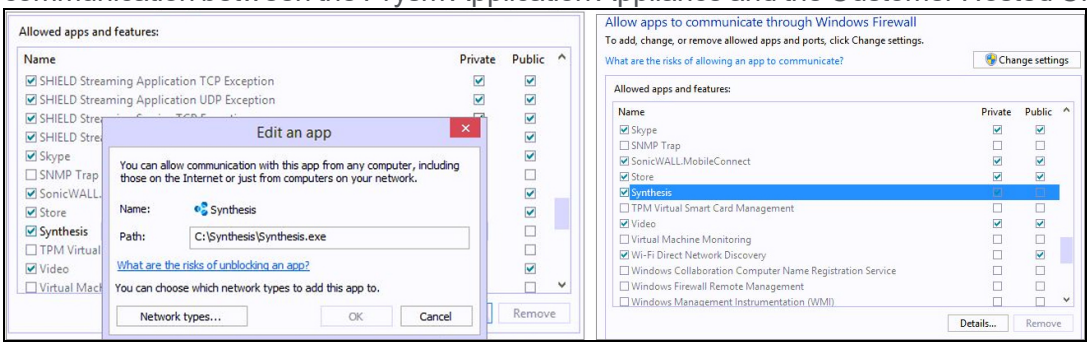
```
! – prysm web-portal
access-list 101 permit tcp host <source ip address> host <destination ip address> eq 4443
!- prysm api communication
access-list 101 permit tcp host <source ip address> host <destination ip address> eq 80
access-list 101 permit tcp host <source ip address> host <destination ip address> eq 443
!- prysm syslog
access-list 101 permit udp host <source ip address> host <destination ip address> eq 5757
!- prysm license entitlement service
access-list 101 permit tcp host <source ip address> host
https://flex1175.compliance.flexnetoperations.com/deviceservices eq 443
```

## Quality of Service (QoS)

For organizations that utilize Quality of Service (QoS) classifications across their private MPLS circuits to branch office, it is recommended to include the Prysm Web API traffic within the 'Business Data' (or higher) Behavior Groups, (i.e., DSCP 26/AF31). The IETF defines the Assured Forwarding behavior in RFC 2597 and RFC 3260.

## Intrusion Prevention/Detection/Proxy-Appliance Services

For organizations that leverage IT security prevention appliances such as an IPS/IDS/Proxy-Server, the Prysm executable (c:\synthesis.exe) must be added to the white-list for proper ASP.net application communication between the Prysm Application Appliance and the Customer Hosted Cloud server.




## Remote Support

Prysm Technical Support Engineers use 3rd-party remote-support software such as Bomgar and/or LogMeIn. For IT security purposes, these are "attended-access" authorized and monitored by the customer. For more information regarding network ports requirements, please reference the vendor websites as network requirements may change.

- Bomgar: https://www.bomgar.com/docs/privileged-access/getting-started/deployment/dmz/ports-firewalls.htm
- LogMeIn: https://secure.logmein.com/welcome/webhelp/EN/CentralUserGuide/LogMeIn/c_lmi_firewalls.html