

# ScreenScape Networks

Service Requirements for Restricted Networks  
1st Generation Connect Device

**03** Introduction

**03** Whitelisting

**04** Third Party Content

**05** IP and Ports

# Introduction

This information is provided to allow Network Security resources to understand and configure Network policies to allow access to ScreenScape Services over restricted networks. This information is subject to change without notice. It is recommended to configure whitelists by url names over IP address to limit the risk of changes impacting functionality.

## Whitelisting

We recommend that a whitelist rule be configured for \*.screenscape.com for both http/https protocol to allow access to the full suite of ScreenScape services.

### ScreenManager Service Requirements (Online Application)

The ScreenManager application should be open to \*.screenscape.com for both http/https.

#### Specific URLs

- http://www.screenscape.com
- https://www.screenscape.com
- http://manage.screenscape.com
- https://manage.screenscape.com
- http://hostedvideo.screenscape.com
- https://hostedvideo.screenscape.com
- http://cdn.screenscape.com
- https://cdn.screenscape.com
- http://support.screenscape.com
- https://support.screenscape.com

## SmartPlayer Service Requirements (Device Software)

The ScreenScape Connect (1st Generation) should be open to \*.screenscape.com for both http/https.

### Specific URLs

- http://manage.screenscape.com
- https://manage.screenscape.com
- http://hostedvideo.screenscape.com
- https://hostedvideo.screenscape.com
- http://cdn.screenscape.com
- https://cdn.screenscape.com
- http://deploy.screenscape.com
- https://deploy.screenscape.com
- http://messagingstorage.screenscape.com
- https://messagingstorage.screenscape.com
- http://google.com
- https://google.com

*Network Time Protocol (NTP) will be from \*.pool.ntp.org*

## Third Party Content

The ScreenScape service includes support for third party content services, such as YouTube and RSS. These services are available through ScreenScape on devices with unrestricted Internet access. Customers operating restricted networks, who wish to access third party content will need to add the necessary network rules, as determined by them for the content they wish to access, for third party content to function normally.

# IP and Ports

If IP Port based rules are required, use the following:

## ScreenManager Service

IPv4 Range	Port
65.17.211.192/26	TCP/80
65.17.211.192/26	TCP/443
Please add IP Address for AWS CloudFront and S3 <a href="http://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html#aws-ip-download">http://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html#aws-ip-download</a>	TCP/80

## SmartPlayer Devices

IPv4 Range	Port
65.17.211.192/26	TCP/80
65.17.211.192/26	TCP/443
Please add IP Address for AWS CloudFront and S3 <a href="http://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html#aws-ip-download">http://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html#aws-ip-download</a>	TCP/80
*	UDP/123

*Network Time Protocol (NTP) will be from \*.pool.ntp.org*