ObservePoint

AUTHENTICATION TECHNICAL GUIDE

AUTHENTICATION METHODS
FOR AUDITING SECURE CONTENT

Authentication Methods for Auditing Secure Content

Allowing ObservePoint to audit your QA/staging servers is a critical step in the release cycle for your website. It will enable you to verify that data collection technologies are deployed correctly, before data quality has been affected.

Most enterprise businesses have IT security protocols in place to protect QA/staging servers from unauthorized access. To audit these resources, your IT security group will need to allow ObservePoint access to these protected resources. The following security methods are supported by ObservePoint:

1. Firewall
2. Basic authentication
3. Proxy authentication
4. Reverse Proxy
5. Browser or form-based authentication
6. Private DNS
7. VPN

Note: Secure website addresses provided to ObservePoint must match your SSL Certificates in use by ObservePoint.

1. Firewall

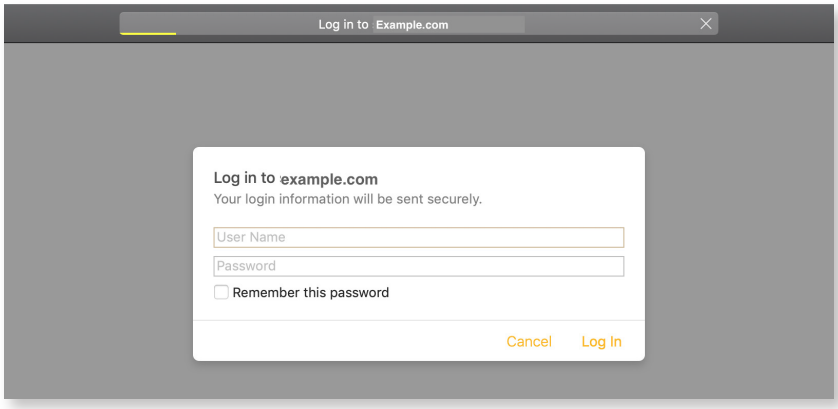
When access is controlled by firewall, instruct your IT security group to allow access to **ports 80** and **443** for the ObservePoint IP addresses. These addresses will be provided for you by your Customer Success Manager.

Note: Using DNS records is the preferred approach as it will continue to work in the event of an IP address change.

2. Basic Authentication

Instead of using firewall security, some businesses will use a server protocol called Basic authentication. This is the case when a browser pop-up requests a username and password before allowing access to any content.

Basic authentication transfers usernames and passwords between the browser and server in unencrypted plain text which can be intercepted. It is our recommendation that all QA/staging servers be secured using a firewall, since this is the most secure way to prevent unauthorized access to these resources.



The URL syntax for basic authentication appends the username and password separated by a colon to the beginning of the URL like this:

https://username:password@https://mysite.com

To audit a site using Basic authentication:

1. Select the checkbox for Record a New User Session in the audit.
2. In the Audit Login Settings screen, enter the login URL with your credentials prepended to the URL:

   https://username:password@https://mysite.com

4. Save the configuration

Note: Best practice for Basic authentication is to use a secure protocol (https://) so that the credentials are not sent in the clear. However, regardless of the URL's protocol, the Basic authentication URL is stored on ObservePoint's servers just like any other URL and is not encrypted. By specifying _https_the ObservePoint browser will create a secure connection with your server and send the credentials in encrypted text.

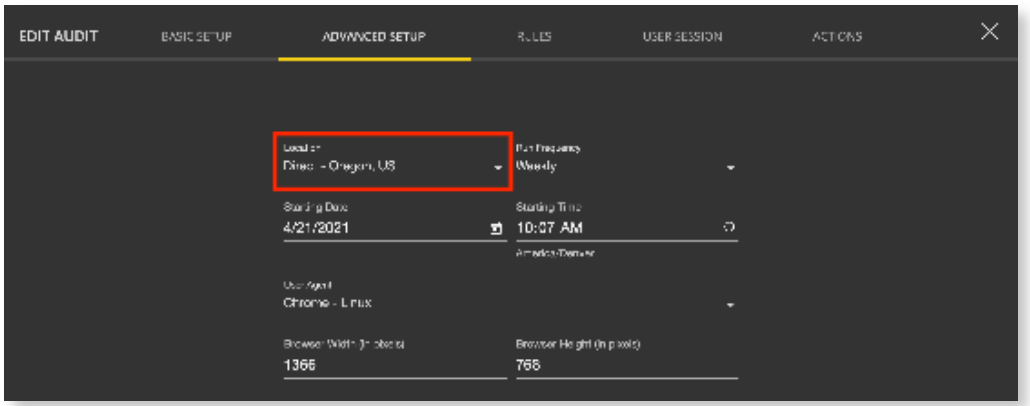
3. Proxy Server

Some QA/staging servers are accessible via a custom web proxy. If this is the case, you will need to configure the audit or user journey to utilize your custom proxy and any additional authentication you may have.

Your web proxy must be internet accessible, and ObservePoint's IP addresses must be **whitelisted**.

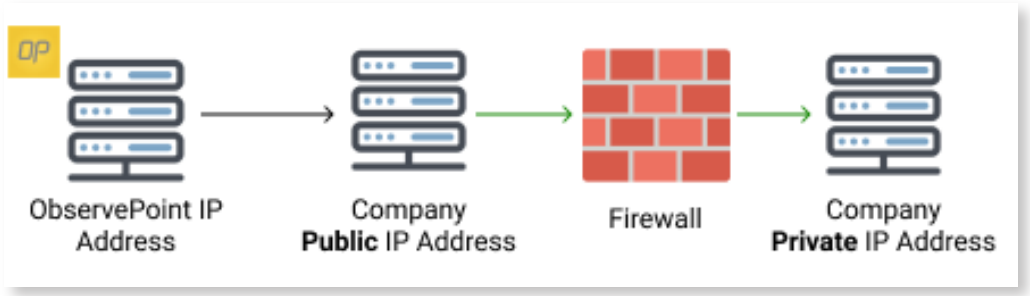
To audit a site via a custom web proxy:

1. Set up your audit as normal and then select Advanced Setup
2. Under Location, select use a custom proxy
3. Input the proxy in the format required (e.g. http://example.com:8080)



4. Reverse Proxy

One way ObservePoint can access staging/QA environments is through Reverse Proxy. In simple terms, using Reverse Proxy, our servers make a request to a publicly accessible server owned by your organization and then your organization forwards the request to an internal server as shown in the diagram below.



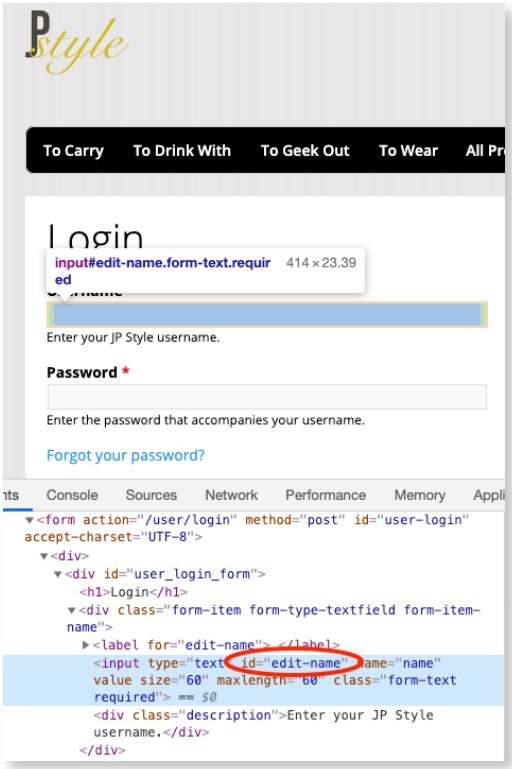
To set up access for an internal, pre-production environment, ObservePoint will need the IP address of your reverse proxy server. Your IT team will need to know that the request will come from one of these ObservePoint IP Addresses.

If your team configures the reverse proxy server for all the **ObservePoint IP addresses**, then audits or journeys can use any of the available proxies, but only the Direct-Oregon, US IP address (35.161.29.125) is really necessary since the origin of the original request will get lost in the handoff.

5. Browser or Form Based Authentication

Form-based authentication uses a login like your email or banking website.

Using form-based authentication with ObservePoint requires each field to have a unique HTML ID or other type of selector. The image below shows the username field has an ID of "**edit-name**".



Under the User Session tab add **Actions** to fill in the username and password fields and to click the Submit button. You can also create an **Action Set** which allows you to save your login to use for several audits.

6. Private DNS

ObservePoint can access your sites that are publicly accessible, yet not publicly known, when you provide ObservePoint with the private DNS entries for your websites. When ObservePoint adds your private DNS entries to its host files it will be able to resolve siteA.yourcompany.com to your IP address.

Note: This may need to be used in conjunction with whitelisting ObservePoint's IP addresses.

7. VPN

Access through VPN is a custom service with additional costs. ObservePoint will work with your network administrators to verify that VPN is an option for your company and will need basic information to evaluate and scope the solution, including:

1. Primary network contact name and email
2. Type of firewall in use (Cisco, Juniper, etc.)
3. Connection timeout, if any
4. Firewall public IP
5. Firewall test credentials: username, password, group name, group password, security token, etc.
6. URL of sample internal website and any site credentials. These websites must be accessible using DNS entries rather than direct IP address, to prevent any conflicts with overlapping IP ranges between your network and ObservePoint's network.

Note: The ObservePoint VPN account needs to allow for local LAN access so that it can communicate simultaneously with your network and ObservePoint's network. ObservePoint's servers will not connect to the outside internet while connected to your network.

There is a cost associated with setting up a VPN. Please contact your Consultant to initiate a custom plan for this service.