Guidelines for Implementing a Custom Domain Name

First-party tag delivery with Ensighten is designed to be easy to use and easy to set up. To protect yourself from ad blockers that can incorrectly categorize *nexus.ensighten.com* as a malicious domain, we strongly recommend implementing or migrating to Ensighten's first-party tag delivery network (TDN). After successfully deploying first-party tags on Ensighten's TDN – all Manage related requests are sent to a new domain of your choosing, for example, *agility.customerdomain.com* instead of the default third-party *nexus.ensighten.com* domain.

You can have a single Ensighten tag management custom domain name configured for your Manage account including multiple websites with different root domains. That is, the *Bootstrap.js* file is considered first-party from the primary organization domain, but third-party from the other organization-owned domains. This is a single TMS domain configuration and it is the fastest, simplest and least expensive to setup and maintain.

Ensighten's first-party TDN supports other configurations, including multiple SSL certificates for different custom domain names or multi-domain subject alternative name (SAN) SSL certificates. For example, a single SAN certificate can provide full first-party support across multiple websites that have different root domains.

You can deploy a SAN certificate instead of a standard single domain certificate. We recommend contacting an Ensighten Support representative to better understand the logical and strategic mapping between your websites as they relate to Ensighten's spaces and publishing paths.

Prerequisites

- An organization controlled DNS system and zone for domain name
- An organization owned domain name such as, *customerdomain.com*.
- A subdomain name registered as a CNAME Resource Record in DNS such as, *agility.customerdomain.com*.
- An X.509/PEM format Secure Socket Layer (SSL) certificate signed by a reputable Certificate Authority (CA)
- An organization email you can use for system generated certificate expiration notifications.

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA

***Note**: Completing your first-party migration can take up to 4 weeks.*

Getting Started

To perform first-party implementation or migration you must belong to a role with permissions to Certificates and Publish Paths as well as the admin user role.

***Note**: Make sure to log out and log back in after new roles are added to activate the updated permissions.*

If these roles are not available, contact your Ensighten point of contact or Ensighten Support.

Getting the SSL/TLS Certificate

Ensighten generates a secure 2048-bit RSA private key that is unique to the certificate request. This key is used to sign a text file known as a Certificate Signing Request (CSR) that Ensighten generates based on a set of attributes supplied by your organization, including the Custom Domain Name that you choose.

Once generated, you can download the CSR file from Manage UI to procure an SSL certificate from a recognized CA. Ensighten retains the private key associated with the certificate.

Only the Ensighten server nodes can use the certificate and key to sign and encrypt traffic. Your organization retains control over the certificate including full revocation rights and is responsible for maintaining its validity for the lifetime of its use.

Required X.509 Attributes

Collect the following information using your organization's policies and procedures for procuring an X.509/PEM format server certificate. Ensighten uses this information to correctly generate a valid CSR for your new certificate.

***Note:** The values you supply must match exactly with the values that your organization previously supplied to its CA and that your organization's CA has approved. Mismatched values can cause delays in the process and require generating a new CSR with the correct values.*

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA

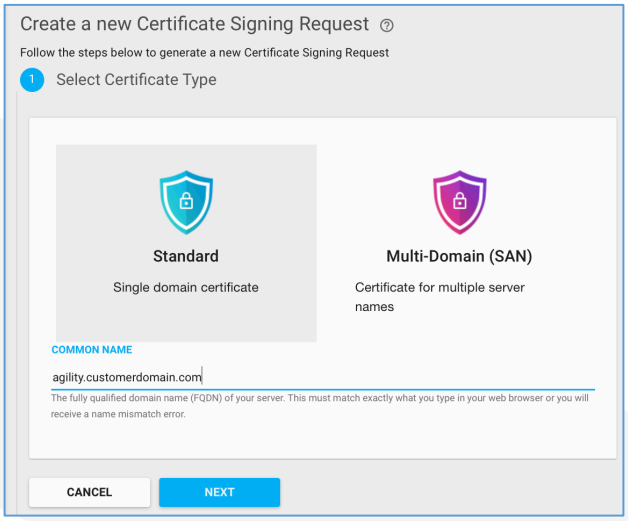
- **CN** (common name): Custom domain name, example agility.customerdomain.com.
- **OU** (organizational unit): Blank or the name of the division in your organization that will manage the certificate.
- **O** (organization): The full, legal name of your organization without abbreviations such as LLC or Inc.
- **L** (Locale/City): The name of the city where your organization is located.
- **S** (State/County/Region): The complete name of the state, county or region where your organization is located.
- **C** (Country code): The two-letter code for the country where you organization is located.

Note: *Your organization may require additional attributes above and beyond those noted to procure a certificate. Ensighten may be able to honor extended attributes as required – but note that in this case you'll need to contact Support to assist with your CSR generation as opposed to having one automatically generated via the self-service Manage UI. When contacting Ensighten Support for this please include the standard attributes as well as the full extended attribute names and values.*

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA

Generate a New CSR from Manage

1. Choose a certificate type and common name:
   - A **Standard** certificate for a single domain.
   - A **SAN** certificate for multiple server names.
     - **Common Name**: Provide all FQDN (fully qualified domain name) including alternate names of your servers.

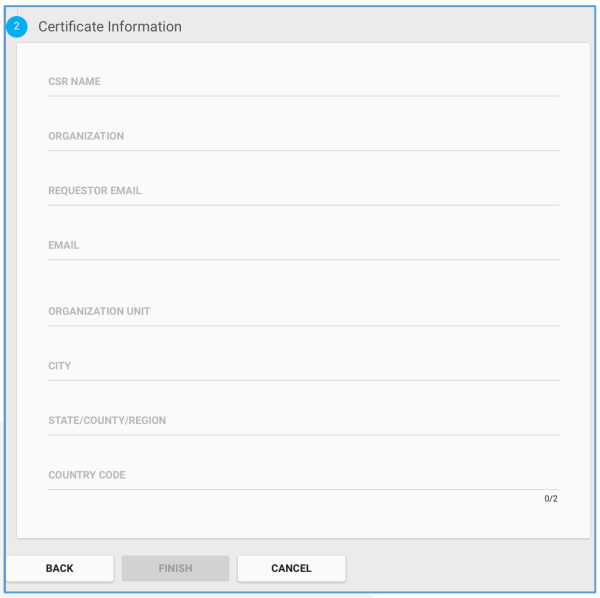


***NOTE**: Do not include the protocol (http/https) in the domains you provide.*

Click **NEXT**.

2. **Certificate Information**: Type the X.509 information you collected into the form.

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA



Click **FINISH**.

3. Follow your organization's policies and procedures for submitting the CSR to a recognized CA. Once the CSR is submitted, your organization's CA will verify and use it to generate an SSL certificate based on your organization's requirements.

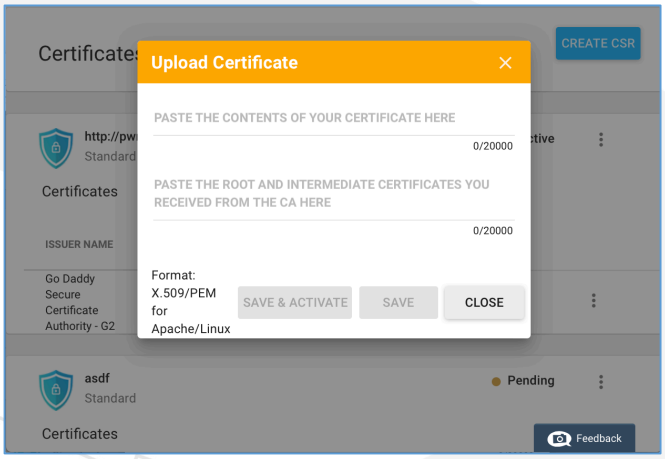
   Note *that the certificate files obtained should be X.509/PEM format and compatible with Apache/Nginx/Linux servers, NOT Microsoft servers such as IIS or Exchange.*

Upload a Certificate

After submitting the generated CSR, the signed SSL certificate is returned in PEM files by your trusted CA.

1. Prepare the signed certificate for upload by opening all the files with extension *.crt* or *.pem* you received with a text editor. Make sure you include intermediate and root certificates which will be located below the primary certificate.
2. Copy and paste in the following order and save the combined data as a *.pem* file.
   i. Primary SSL Certificate
   ii. Intermediate Certificate
   iii. Root Certificate

   You can now upload the contents of the *.pem* you created to the Ensighten server.
3. To upload, slide across the row and click **MORE** and choose **Upload Certificate**. Copy and paste the full contents from the text editor into the form in the order:
   i. Primary SSL Certificate: the first input field contains the custom domain name
   ii. Intermediate Certificate
   iii. Root Certificates.



Click **SAVE & ACTIVATE** and the certificate appears with status **Active** on the certificate list page.

***Note**: Selecting **SAVE** alone does not activate the certificate. You must manually activate the certificate later.*

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA

Once activated, allow 5 up to 10 minutes before navigating to Publishing Paths area of Manage. This gives enough time to automatically create the necessary DNS records and synchronize the certificate files to all TDN nodes.

Note: *Some CAs sign certificates using intermediate certificate chains. These certificates may not be widely available in some web browsers such as those on many mobile devices. If your certificate is issued with an intermediate certificate chain, make sure to include all certificates in the chain when submitting your certificate to Ensighten. Ensighten installs the intermediate certificate chain on its servers. Ensighten's servers will supply them to web browser clients during the SSL/TLS handshake process, allowing browsers that do not store these certificates to verify your Custom Domain Name certificate.*

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA

DNS Registration of CNAME

The steps below walk you through registering a CNAME record for use with your Custom Domain Name. A CNAME record is an alias for another domain, it is like call forwarding for internet traffic.

Required Information to register a CNAME record in DNS:

1. The domain name you want to associate with Ensighten Manage, for example, this is the call forwarding example *FROM* location.
2. A specific domain name you want assigned to your Ensighten Manage account, for example, this is the call forwarding *TO* location.

Note: *The work of obtaining an SSL certificate and deploying the required CNAME can occur at the same time. You can set up the CNAME record before DNS records are created by Ensighten's systems.*

Register **Custom Domain Name** for use with Ensighten Manage as follows:

Note: *Use your organization's policies and procedures for registering CNAME entries in DNS before attempting these steps.*

1. Obtain a Fully Qualified Domain Name (FQDN) to associate with your Ensighten implementation (example: agility.customerdomain.com). This is your **Custom Domain Name**.
2. Obtain the specific FQDN assigned to your Ensighten Manage instance by taking your Manage account name and adding the following to the end *.edge.nc0.co*. This is your **Assigned Domain Name** for example: *widgetsinc.edge.nc0.co*. You will see this record in the Publishing Paths section of Manage. Your **Assigned Domain Name** is always the same for all certificates used in your Manage account.

   Note: *DNS records do not allow underscore ("_") characters per RFC conventions. If your Manage account name contains an underscore or any other special character, this will be automatically replaced with a hyphen (e.g. widgets-inc.edge.nc0.co instead of widgets_inc.edge.nc0.co).*

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA

3. Use your **Custom Domain Name** and your **Assigned Domain Name** to register a CNAME-type Resource Record in your organization's DNS system.

   Use the **Custom Domain Name** that you choose as the name of the CNAME record and the **Assigned Domain Name** as the target. Example:
   CNAME Resource Record Name = `<agility>.<customerdomain>.com`

Multi-domain SAN Certificates

If using a multi-domain SAN certificate, you must set up a CNAME record for each of the domains in that certificate. Make sure to review your organization's policy on Time-To-Live (TTL) settings for DNS Resource Records. The TTL that you choose determines how long caching DNS resolvers on the Internet wait before requesting an update for your CNAME record.

- Lowering the TTL increases the frequency of requests to your organization's DNS system.
- Increasing the TTL reduces the frequency of requests to your organization's DNS system.

***Note**: Ensighten recommends using a TTL that is less than or equal to 15 minutes.*

If you intend to implement your own Resource Record failover, you can lower TTLs to within the 1-5 minute range.

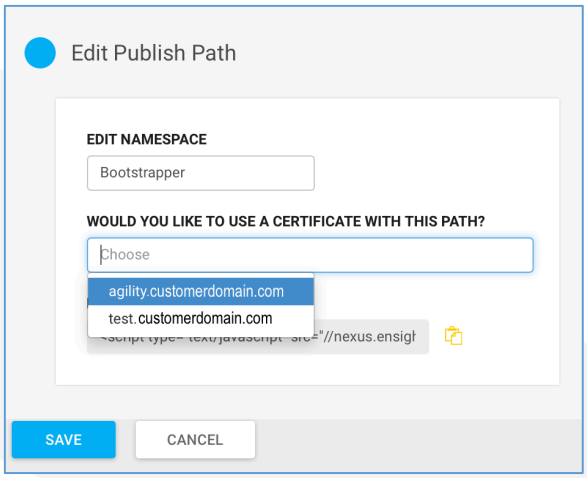
***Note**: Ensighten's TDN implements TTLs of 2 minutes for failovers.*

Different DNS client resolvers have different behaviors for handling TTLs on CNAME records, for some clients, the TTL value you choose for your CNAME record can place a lower bound on the amount of time required for clients to be redirected to healthy Ensighten tag serving nodes in failover scenarios.

Publishing Paths to Certificate Mapping

When the SSL certificate is successfully installed on Ensighten's TDN – and your required CNAME record is in place – the next step is providing Ensighten with a mapping for **Custom Domain Names** associated with your publishing paths, that is, the *Bootstrap.js* files. Use Manage to perform this update.

1. Navigate to **Publishing Paths** and then for each publishing path – select the **Edit** option.
2. Type the JavaScript namespace you want for this Bootstrap file. In most cases, this field does not change from the default value of Bootstrapper.



3. Associate one of your **Custom Domain Names** or certificates with this publishing path from the drop-down list. Leaving this field blank uses the default third-party, *nexus.ensighten.com*.
4. Click **SAVE** to return to the publishing paths list page. Edit the next publishing path until finished.

***Note**: No changes take place in your generated code and implementation until you publish the spaces/Bootstrap.js files.*

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA

Pre-Bootstrap Update Testing

Make sure your CNAME is correctly set up and your SSL certificate is correctly installed. Additionally, you can have someone familiar with testing DNS records make sure that everything resolves correctly. (Use the `DIG` command at the terminal to do this work.).

You can use a packet sniffer such as Charles or your browser network monitor on website traffic to make sure that Bootstrap files are still pointed to the third-party *nexus.ensighten.com* location and functioning as expected.

You will see the initial *Bootstrap.js* file request go to *nexus.ensighten.com*, but then all calls after, such as the *serverComponent* and the async page-specific code files go to the new Custom Domain Name associated with this *Bootstrap.js file*.

If you notice anything different, contact Ensighten Support for assistance.

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA

Update on-Page Bootstrap.js File References

When you edit the publish path, there are 2 Bootstrap file references.

1. The legacy reference to nexus that should already be deployed on your pages if you are in a migration scenario.
2. The new reference that uses your Custom Domain Name. All on-page *Bootstrap.js* file references on your websites should be updated to use the appropriate domains.

If your Ensighten architecture strategy calls for a single Custom Domain Name across all websites and pages – update the Bootstrap URLs everywhere to that new single value.

If your Ensighten architecture strategy calls for various **Custom Domain Names** using a multi-domain SAN certificate, you must make sure the right Bootstrap URLs are updated to the corresponding values across all websites and webpages.

The Ensighten first-party TDN is designed to work flawlessly across situations where the *Bootstrap.js* file references on your website are not able to be updated simultaneously. Even if one page is pointing to *nexus*, and the next page is pointing to your new **Custom Domain Name**, everything continues to work as expected. Given this flexibility, Ensighten recommends starting the process of getting all third-party nexus-pointing Bootstrap.js files updated to use your new **Custom Domain Names** – but you don't need to worry about the timing of when this effort is completed with one major exception: **DO NOT** begin updating your on-page Bootstrap URL references until **AFTER** the relevant SSL/TLS certificate(s) are installed, the CNAME records deployed, and all carefully tested and found functioning properly.

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA

Post-Bootstrap Update Testing

Once your on-page *Bootstrap.js* file URLs are updated to point to your Custom Domain Name, you should test again using a packet sniffer to make sure all Ensighten related requests are being successfully sent to your Custom Domain Name. If you see anything that causes concern, contact Ensighten Support for assistance.

Important Notes

Ensighten's first-party TDN was primarily developed to support Manage and related tag management specific efforts. Some Ensighten products such as Pulse already support first-party requests. It might be feasible to implement using the same domains and certificates across multiple products. Other Ensighten products such as Mobile or Privacy may not support first-party use cases initially. In this case, they will continue to use the default *nexus.ensighten.com domain*. If you have specific requests or want more information, contact Ensighten Support.

Note: *First-party requests are not compatible, by design, with the commit-based nexus-test serving infrastructure as this would greatly increase the cost and time required to setup and maintain the solution with potential benefits being negligible. When using nexus-test (using Charles rewrites or the Ensighten developer tools plugin) you'll want to have the Bootstrap.js file reference point directly to nexus-test.ensighten.com to be able to complete your local testing.*

As of the initial release of Ensighten's first-party TDN, e.gif beacons, performance beacons and tag audit beacons are still sent directly to *nexus.ensighten.com* and not yet updated to use your Custom Domain Name. It is important to remember that this state does not harm anything and Ensighten plans to address this issue soon.

Finally, the Ensighten Developer Tools browser plugin has also not been updated to work with your Custom Domain Names, however, this will be addressed shortly as well.

Ensighten | info@ensighten.com | Confidential Fax: 650-887-2575 | T:650-249-4712
226 Airport Parkway | Suite 390 | San Jose | CA 95110 | USA