HFHS Adding New Domains

Issuing New SSL Certificates

When do I need this?

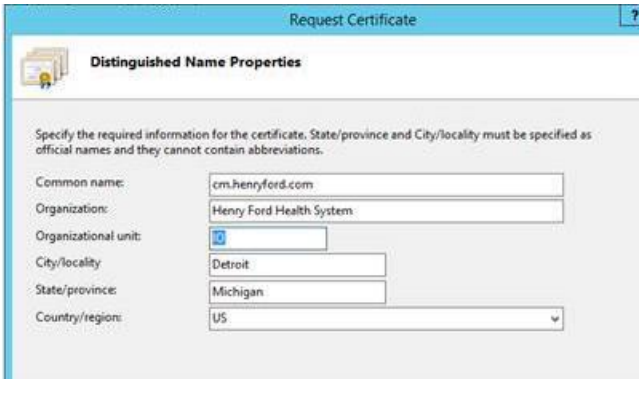
This will be needed in the following situations:

1. New, distinctive domain that warrants having its own SSL certificate
2. The alternative domain names threshold has been reached on the existing SAN certificate
    a. SAN certificates do have limitations on the number of alternative names that can be associated. This will depend on the certificate vendor.
    b. Please confirm with your certificate vendor on the exact number and keep this number handy for future domain request
    c. If the alternative name threshold has been met, you will have to purchase and issue a new SAN certificate
3. A new vanity domain is desired but the alternative domain names threshold had been reached on the existing SAN certificate
    a. Even though the request is for a vanity domain, you must still associate the domain to an SSL certificate if you want HTTPS resolution

Client Prerequisites:

1. **Point of contacts** – Confirm the point of contacts for general DNS/certificate correspondence, zip cert files, meeting coordination, etc
2. **DNS entry for domain** - Confirm that you have a DNS entry for the domain(s) you would like to issue the certificate for
    a. Coordinate with your DNS vendor if you do not already have an entry
3. **Name properties** - Confirm the Distinguished Name Properties standards for the HF organization
    b. Typically the organization will require uniformity in any digital certificates that are issued
    c. Any new certificate issues should follow the organization's convention

Here's a mockup of what these Distinguished Name Properties could be. PLEASE confirm the HF organization's standards for these properties since each organization may have different requirements/rules (these are ONLY mockups).



4. **Key Type** and **Hash Algorithm** – These will be RSA and SHA256 respectfully
    a. If your SSL certificate vendor/the HF organization would like this changed due to a special need, please let us know
5. **Bit Length** – Confirm the minimum bit length for the key used by the SSL certificate
    a. Your SSL certificate vendor will inform you the required length

   b. Bit length used by the SSL certificate correlates to the security encryption level of the certificate (longer = more secure)
   c. The current standard is 2048, but *PLEASE* reconfirm this each time you purchase a new certificate or make modifications to an existing certificate
6. **Environment** – Confirm the environment this new domain and certificate are for
   a. Will this just be a Production-ONLY request?
   b. Will this also require a corresponding TEST (non-Production) domain as well?
   c. This will depend on the use case
   d. MedTouch can help determine if a TEST domain would be recommended. For example:

a. Many organizations use a unique domain for their blogs (www.henryford.com VERSUS [HFblogname].org).

7. ii. While the production domain will be set up (ex: [HFblogname].org), we would recommend creating a parallel non-production domain for lower environment testing rather than just leveraging the primary site domain (ex: t[HFblogname].org versus twww.henryford.com/[HFblogname])

MedTouch Prerequisites:

1. **IP addresses** - Based on the **Environment prerequisite (#5),** we will provide the IP address(es) associated for each new domain
   a. You will provide this information to your DNS vendor

What happens next?

1. Once MedTouch has **client prerequisite 1 -5**, we will confirm the timeframe for:
   a. Generating the CSR
      i. Standard = 3 business days
      ii. RUSH = to be coordinated based on client's target timeframe (will incur additional costs)
   b. MedTouch's ideal turnaround time for actual issued SSL certificate to arrive
      i. We will note who they should be sent directly to (via secure email)
   c. Based on when the SSL certificate arrives, when the updates will be made for the relevant environments
      a. Standard = will be processed during the upcoming deployment/release window RUSH = To be coordinated based on client's target timeframe (will incur additional costs)
   d. When Client Testing/confirmation can begin
2. MedTouch process the request and generate a Certificate Signing Request (CSR) from the webserver the SSL certificate will be placed on.
   a. If more than 1 SSL certificate will be issued, we have to generate a CSR for each of the corresponding certificates
   b. If the SSL certificate will be issued across many webservers, we will generate a CSR for each webserver (e.g. Production and Non-Production environment using the same SSL certificate)
3. MedTouch will send the generated CSRs via secure email to the **Point of Contact (#1)** and communicate target turnaround time for the actual SSL certificate to be sent to MedTouch.
4. The Client will submit the CSR(s) to your Certificate vendor and request the full SSL certificate.
5. Once the certificate vendor has approved the request and issued the certificate(s), download the primary and intermediate certificate from the vendor
   a. Your vendor will provide instructions on how to do this – each vendor is unique
6. Please send the primary and intermediate certificates to MedTouch via secure mail
   a. CONFIRM that MedTouch has received the certificate(s)!
7. MedTouch will install the new SSL certificate to certificate store of the relevant environment(s)
   a. This will ensure that when a user makes a request for the domain, the SSL certificate is available for a successful HTTPS redirect
   b. The SSL certificate should be added to the certificate store BEFORE completing #8 and #9 OR at the SAME TIME #8 and #9 are completed
8. MedTouch will subsequently update the webserver environment configuration files to associate the new domain to the appropriate node (if applicable)

    a. This will ensure that whenever anyone makes a request for the domain the URL resolves to node/sub-node that has been indicated in the environment configuration file
    b. This does require a code deployment to the relevant environment
    c. Since this requires update a configuration file, the CM server of the environment will restart
9. MedTouch will add an IIS binding to the domain on the relevant environment(s)
    a. This will ensure that the domain is recognized when the request is made by a user
    b. This does not require a code deployment BUT should be done in parallel to #8 to ensure proper resolution to the correct page
10. MedTouch will confirm proper resolution of the domain/vanity domain
11. MedTouch will inform the client with the domain/vanity domain is ready for use/confirmation on the relevant environment

Adding to existing SSL Certificates

When do I need this?

This will be needed in the following situations:

1. The new domain can be added as an alternative domain names on an existing SAN certificate that has already been bound to the webservers for the environment(s)
    a. SAN certificates do have limitations on the number of alternative names that can be associated. This will depend on the certificate vendor.
    b. Please confirm with your certificate vendor on the exact number and keep this number handy for future domain request
    c. If the alternative name threshold has been met, you will have to purchase and issue a new SAN certificate
    d. If the domain can be added as alternative domain name, MedTouch does not need to generate a CSR since the SSL SAN cert is already on the appropriate webserver(s)
2. A new vanity domain is desired and the alternative domain names threshold has NOT been reached on the existing SAN certificate
    a. Even though the request is for a vanity domain, you must still associate the domain to an SSL certificate if you want HTTPS resolution
    b. If the vanity domain can be added as alternative domain name, MedTouch does not need to generate a CSR since the SSL SAN cert is already on the appropriate webserver(s)

Client Prerequisites:

1. **Point of contacts** – Confirm the point of contacts for general DNS/certificate correspondence, meeting coordination, etc
2. **DNS entry for domain** - Confirm that you have a DNS entry for the domain(s) you would like to issue the certificate for
    a. Coordinate with your DNS vendor if you do not already have an entry
3. **Alternative Name** – Reach out to your Certificate vendor
    a. Request that the new domain (or vanity domain) get added as an alternative name to the existing SSL SAN certificate that is already installed on the designated webserver
    b. Ensure that you are added it to the certificate that corresponds to the matching environment(s)
    c. IP addresses will be the same since the domain is being added to the existing certificate bound to the matching environment(s)
4. **Environment** – Confirm the environment this new domain and certificate are for
    a. Will this just be a Production-ONLY request?
    b. Will this also require a corresponding TEST (non-Production) domain as well?
    c. This will depend on the use case
    d. MedTouch can help determine if a TEST domain would be recommended. For example:
        i. Many organizations use a unique domain for their blogs (www.henryford.com VERSUS [HFblogname].org).

ii. While the production domain will be set up (ex: [HFblogname].org), we would recommend creating a parallel non-production domain for lower environment testing rather than just leveraging the primary site domain (ex: t[HFblogname].org versus twww.henryford.com/[HFblogname])

MedTouch Prerequisites:

1. **None**

What happens next?

1. Once MedTouch has **client prerequisite 1 -4**, we will confirm the timeframe for:
    a. When the updates will be made for the relevant environments
        i. Standard = will be processed during the upcoming deployment/release window RUSH = To be coordinated based on client's target timeframe (will incur additional costs)
    b. When Client Testing/confirmation can begin
2. MedTouch will update the webserver environment configuration files to associate the new domain to the appropriate node (if applicable)
    a. This will ensure that whenever anyone makes a request for the domain the URL resolves to node/sub-node that has been indicated in the environment configuration file
    b. This does require a code deployment to the relevant environment
    c. Since this requires update a configuration file, the CM server of the environment will restart
3. MedTouch will add an IIS binding to the domain on the relevant environment(s)
    a. This will ensure that the domain is recognized when the request is made by a user
    b. This does not require a code deployment BUT should be done in parallel to #2 to ensure proper resolution to the correct page
4. MedTouch will confirm proper resolution of the domain/vanity domain on the relevant environment(s)
5. MedTouch will inform the client with the domain/vanity domain is ready for use/confirmation on the relevant environment(s)