Using Your Own Domain - Vanity URL

> OperationsCommander (OPSCOM) supports the use of vanity URLs, allowing organizations to maintain consistent branding by using their own custom domain for portal access. This article is intended for OPSCOM administrators who wish to configure a custom domain or subdomain for their user and admin portals.

Setup and Configuration

Before beginning, please note that not all service levels include this option and additional fees may apply. Contact your **Sales Representative** at **sales@ops-com.com** for confirmation regarding your account eligibility.

Domain Requirements

You may use any legal and registered domain that your organization owns or controls.

- Domains and subdomains cannot contain spaces.
- Character strings are case-insensitive.
- Subdomains may consist of a combination of A-Z, 0-9, and hyphens.

DNS Configuration

The setup process involves pointing a CNAME record at the OPSCOM server. Refer to the table below for the appropriate DNS entry based on your preferred configuration:

Option	Format	DNS Entry	Notes
1	yourdomain.com	@ CNAME <client>.OPSCOM.com	Points the entire domain to your OPSCOM installation.
2	subdomain.yourdomain.com	subdomain CNAME <client>.OPSCOM.com.	Points a specific subdomain to your OPSCOM installation.

Using this Feature

Once your DNS records are configured, the vanity URL will be used to access your portals.

Resulting URLs

Depending on your chosen configuration, your portal access links will appear as follows:

- **Option 1 (Domain)**:
  - User Portal: **https://yourdomain.com**
  - Admin Portal: **https://yourdomain.com/admin**
- **Option 2 (Subdomain)**:
  - User Portal: **https://subdomain.yourdomain.com**
  - Admin Portal: **https://subdomain.yourdomain.com/admin**

Implementation Process

1. Email **support@ops-com.com** to inform the support team of your chosen registered domain or subdomain.
2. Receive the specific connection details from the OPSCOM team.

3. Add the required **CNAME** record to your organization's DNS settings.
4. Notify the support team once the DNS update is complete.
5. Wait for the installation of a secure **SSL Certificate** (provided via Let's Encrypt), after which your domain will be active.

Best Practices and Considerations

- **Certificate Registration**: SSL security is a requirement. Once your subdomain points to our servers, the certificate request can be processed. **Ensure your IT team is prepared to assist with DNS updates to minimize downtime during this transition.**
- **Planning**: Since this process requires coordination between your IT department and our support team, initiate this request early in your implementation timeline to ensure your branding is ready for your official system launch.

Revision #4
Created 7 October 2024 11:53:15
Updated 2 September 2026 12:37:42