Tenant Specific URL for Webex WFO Users

Version 1.0: 21st November 2025

We're excited to introduce an enhanced tenant-based sign-in experience for Webex WFO - that makes signing in more consistent, secure, and user-friendly.
As part of this roll out, Webex WFO has introduced a dedicated subdomain for each tenant (for example, https://yourtenant.calabrio.one). The unique subdomains are now available within the product.

Accessing Your Subdomain URL (Tenant Specific URL)

Subdomain URLs are now live and available in the product. Administrators can easily find their assigned subdomain under Application Management. The steps to access it are outlined below.
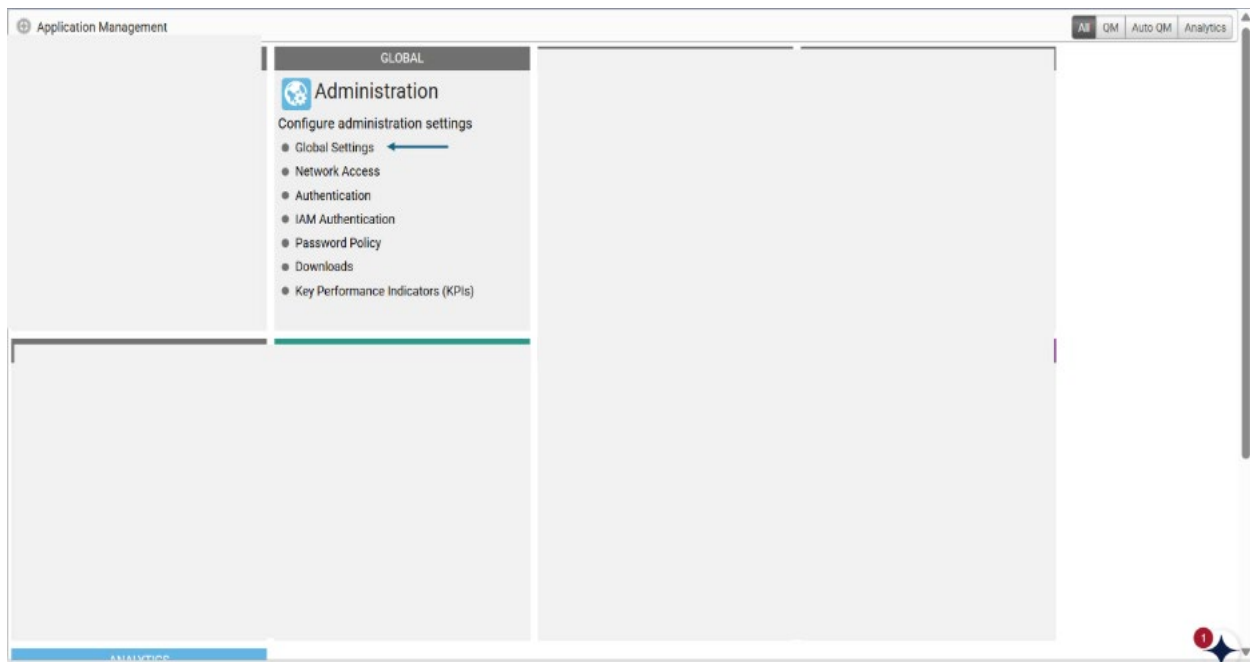
Steps to get your Subdomain URL

Note: Only administrators can access the subdomain information.
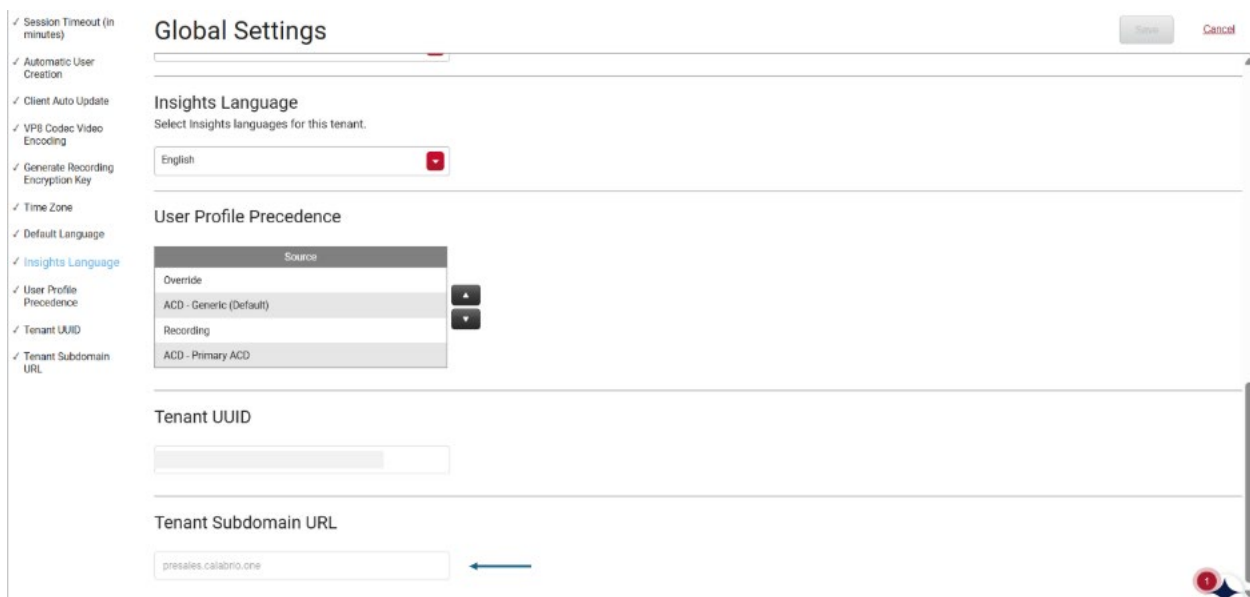
Step 1: Click on Application Management

Step 2: Under Administration, click on Global Settings

Step 3: Scroll down to Tenant Subdomain URL

You can find your system-generated subdomain under Tenant Subdomain URL in the product. Administrators are responsible for sharing this subdomain with their users and updating any related internal documentation. For configuration guidance, please refer to the steps outlined in the page below based on your current sign-in method.
Note: https://wfohelp.com/doc/Content/user-guides/getting-started/first-time-log-in-new.htm

Transition to Tenant Specific Sign-in URLs: What to Expect and How We Support You

Who Benefits from This Change?

All Webex WFO tenants will benefit from these enhancements, with the following exceptions:

- WFM Administrator Client: No changes. Continue using the existing login URL: https://windows.cloud.microsoft/
- WFM Mobile App: No changes to the current login process.

What's Changing?

- **Calabrio Identity Service** will be enabled as the new authentication platform for all tenants.
- Each tenant will have a unique tenant specific subdomain in the format: https://<yourtenant.calabrio.one>
- All users, except WFM Administration Client users, will sign in through Calabrio Identity Services.
- Legacy login paths will remain available during the transition period.
- Users will have access to self-service password reset and account unlock features via Calabrio Identity Services.
- As part of the transition to Calabrio Identity Services, the "welcome emails" feature will be deprecated.

Actions Required for Administrators

To ensure a smooth transition, administrators should:

1. Whitelist the Domain: Work with your IT team to whitelist *.calabrio.one.
2. Locate Your Tenant URL: Find your unique tenant-specific URL within the product interface.
3. Identify Your Sign-In Type: Determine your sign-in flow and authentication type.
4. Follow Configuration Steps: Refer to the resources below for detailed instructions and best practices.

Refer to the resources in the following sections for step-by-step instructions to ensure a smooth, seamless transition.

Parallel Sign-In Paths

To ensure a smooth transition, both the current and new sign-in paths will remain available and operate in parallel for the foreseeable future.

# How to Identify your Sign-in Flow and Respective Configuration

There are four types of sign-in configurations. Follow the steps that match your current setup:

Direct Login Tenants (Legacy)

Administrators can determine the sign-in method in use by checking their current URL and the corresponding authentication setting in Webex WFO.
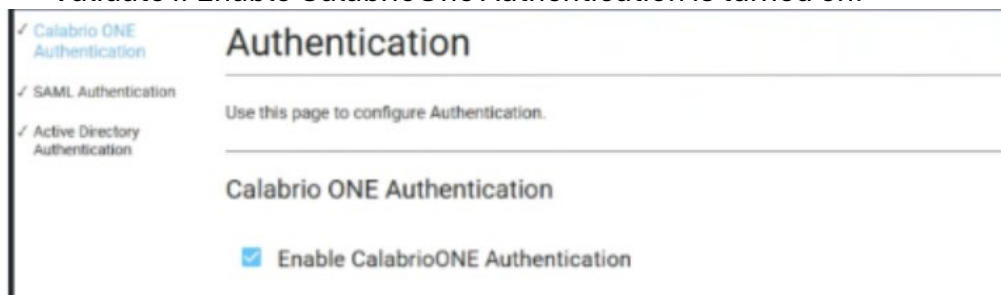**Example URL:** https://us3.calabriocloud.com/#/
Note: This is not login.calabriocloud.com
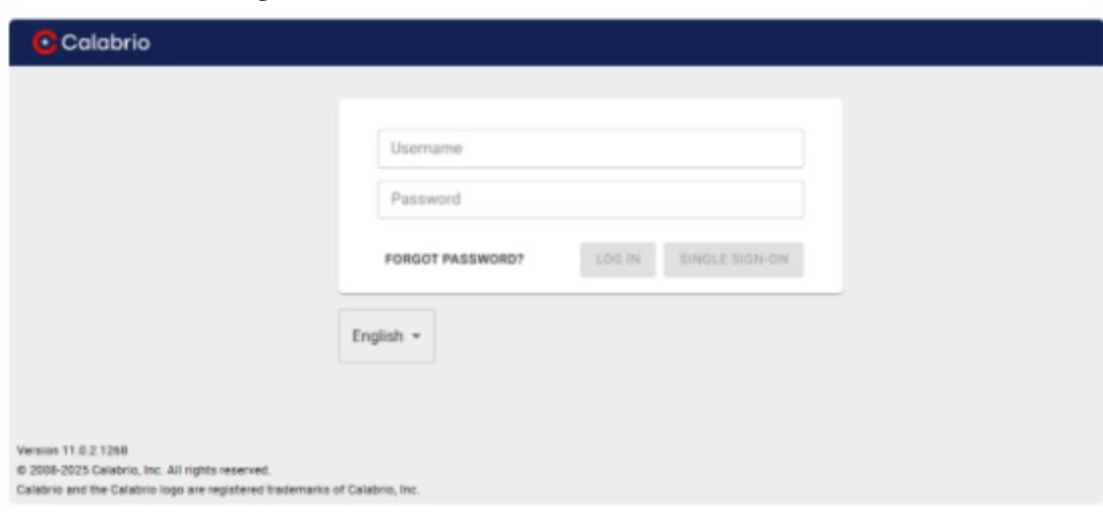
Administrator Setting:
- Navigate: Webex WFO > Application Management > Administration > Authentication
- Validate if Enable CalabrioOne Authentication is turned on.

Note: If the steps above align with your current sign-in process, this is your login flow.

Direct Login Tenants (Legacy) Configuration

Configuration for Tenant Administrators:
What to do:
- Work with your IT team to whitelist *.calabrio.one so the new login subdomain is accessible.
- Configure IAM Direct Login in Webex WFO to support the transition. Help can be found here.

IAM Authentication

SAVE | CANCEL

✓ Enable Authentication

✓ IAM Authentication Settings

Configure the connection between your IDP and the Calabrio ONE IAM service.

Enable Authentication

☑ Enable IAM Authentication (Direct Login)

☐ Enable SAML Authentication (Company Login)

IAM Authentication Settings

Multi-factor Authentication

☐ Enable One-Time Password via Email

- Communicate the new subdomain URL (e.g., https://yourtenant.calabrio.one) to all users.
- Update internal documentation and training materials.

Password and Login Sync Notes:

- Login IDs will sync to the new path after IAM is configured.
- Passwords will sync from legacy to the new process
- Passwords changed in IAM will not sync back to Legacy.
- Password sync may be impacted if the password does not meet IAM policies.

Direct Login Tenants (IAM)

Administrators can determine the login method in use by checking the login URL and the corresponding authentication setting in Webex WFO.
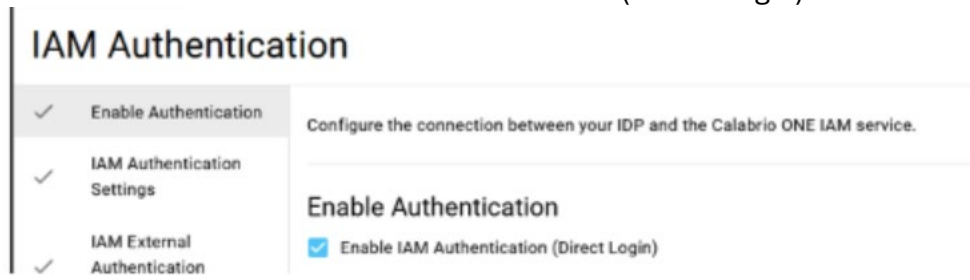**Example URL:** https://login.calabriocloud.com

Administrator Setting:
- Navigate: Webex WFO > Application Management > Administration > IAM Authentication
- Validate if 'Enable IAM Authentication (Direct Login)' is turned on.

Note: If the steps above align with your current sign-in process, this is your login flow.

Direct Login Tenants (IAM) Configuration

Configuration for Tenant Administrators
What to do:
- Work with your IT team to whitelist *.calabrio.one.
- No configuration is needed in Webex WFO.
- Communicate the new subdomain URL to all users.
- Update internal documentation and training materials.
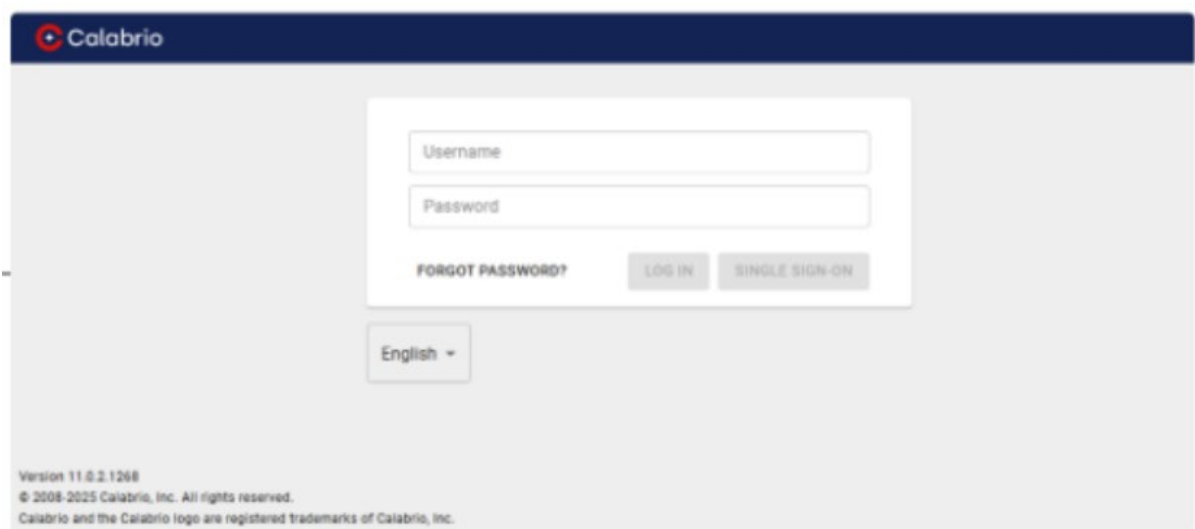
Password and Login Sync Notes:
- Login IDs and passwords remain the same between current and new paths.

SAML/SSO Login Tenants (Legacy)

Administrators can determine the sign-in method in use by checking the login URL and the corresponding authentication setting in Webex WFO.
Example URL: https://us3.calabriocloud.com/#/
Note: This is not login.calabriocloud.com

Administrator Setting:

- Navigate: Webex WFO > Application Management > Administration > Authentication
- Validate if 'Enable SAML Authentication' is turned on

Note: If the steps above align with your current sign-in process, this is your login flow.

SAML/SSO Login Tenants (Legacy) Configuration

Configuration for Tenant Administrators:
What to do:

- Work with your IT team to whitelist ***.calabrio.one**.
- Configure your identity provider (IdP) to support SAML/SSO with the new subdomain login path.
- Administrators will need to configure IAM Direct Login to enable the transition. Help can be found here.

- Communicate the new subdomain URL to users.
- Update internal documentation and training materials.

Password and Login Synchronization Notes:
- Login IDs will synchronize once IAM Direct is configured.
- Passwords are managed by your IdP and not synced by Webex WFO.
- For users with multiple tenants, configure your IdP with a shared SAML application or assign unique email aliases (e.g., john.doe+sales@domain.com)

SAML/SSO Login Tenants (IAM)

Administrators can determine the login method in use by checking the login URL and the corresponding authentication setting in Webex WFO.

Example URL: https://login.calabriocloud.com

Administrator Setting:
- Navigate: Webex WFO > Application Management > Administration > IAM Authentication
- Validate if either of the check boxes under 'Enable Authentication' are turned on

IAM Authentication

Enable Authentication	Configure the connection between your IDP and the Calabrio ONE IAM service.

Enable Authentication

☐ Enable IAM Authentication (Direct Login)

☐ Enable SAML Authentication (Company Login)

Note: If the steps above align with your current sign-in process, this is your login flow.

SAML/SSO Login Tenants (IAM) Configuration

Configuration for Tenant Administrator:
What to do:
- Work with your IT team to whitelist ***.calabrio.one**.
- No configuration is needed in Webex WFO.
- Communicate the new subdomain URL to users.
- Update documentation and training materials.

Password and Login Sync Notes:
- Login IDs remain consistent.
- No password synchronization is required

Need Support?

For any support or questions on tenant specific URL, please reach out to Cisco Support Team.