# Feature Description Document

## Configuring Single Sign-On

# Purpose

This document outlines the process of configuring SSO in IXM WEB.

# Applies to

| TITAN | TFACE | TOUCH 2 | SENSE 2 | MERGE 2 | MYCRO |
|---|---|---|---|---|---|
| All Devices | All Devices | All Devices | All Devices | All Devices | All Devices |

# Description

Single Sign-On (SSO) is an authentication method that enables users to securely authenticate multiple applications and websites by using just one set of credentials. With this feature, IXM WEB users can log into IXM WEB using their Windows credentials.

This document will describe all the available settings and configurations for using the SSO feature in IXM Web.

# Configuring Windows Authentication

1. Once IXM WEB is installed, go to the "**Invixium**" path in the machine where IXM WEB is installed.
2. Navigate to **IXM WEB** >> **Areas** >> **SingleSignOn** >> **Views**.
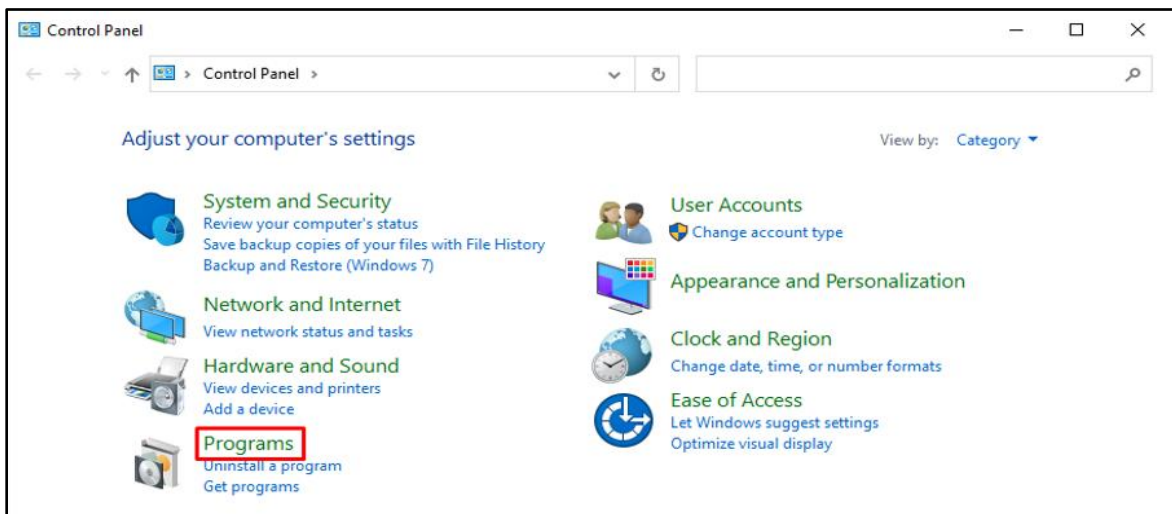3. Open the **web.config** file in any text editor >> Search for "**<system.web>**" >> Add the below text in between "**<system.web>**" and "**</system.web>**":
   <authentication mode="Windows" />
   <authorization>
   <deny users="?" />
   </authorization>
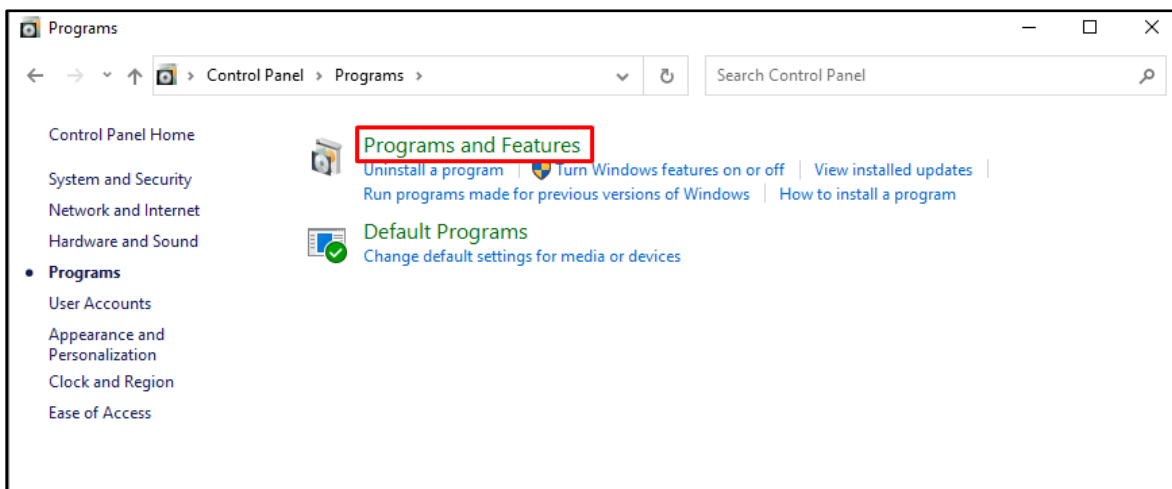


4. Save the "**web.config**" file.

# Enabling Windows Authentication

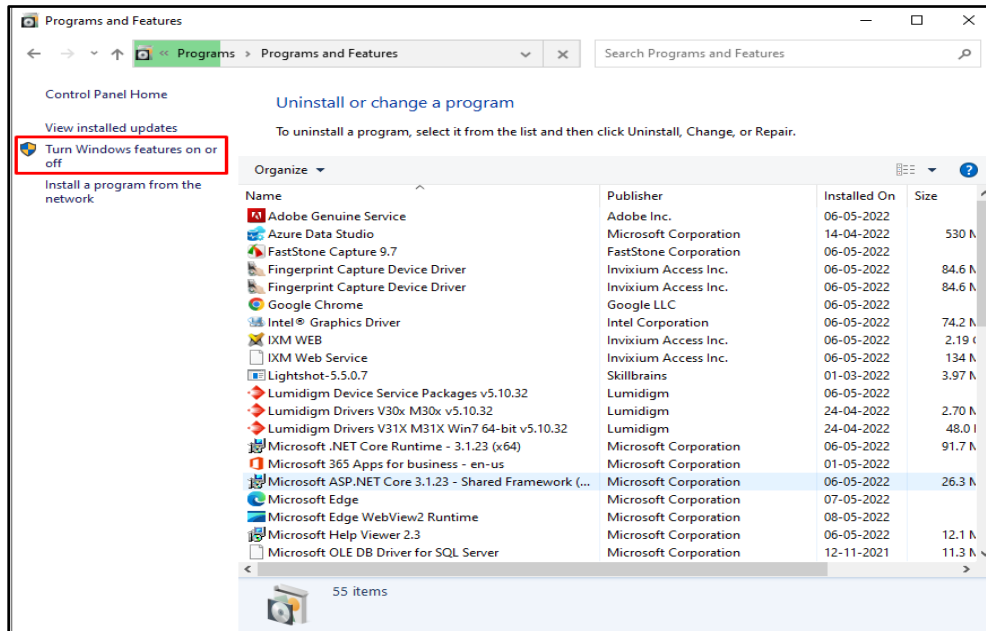## a) Enable Windows authentication from the Control Panel

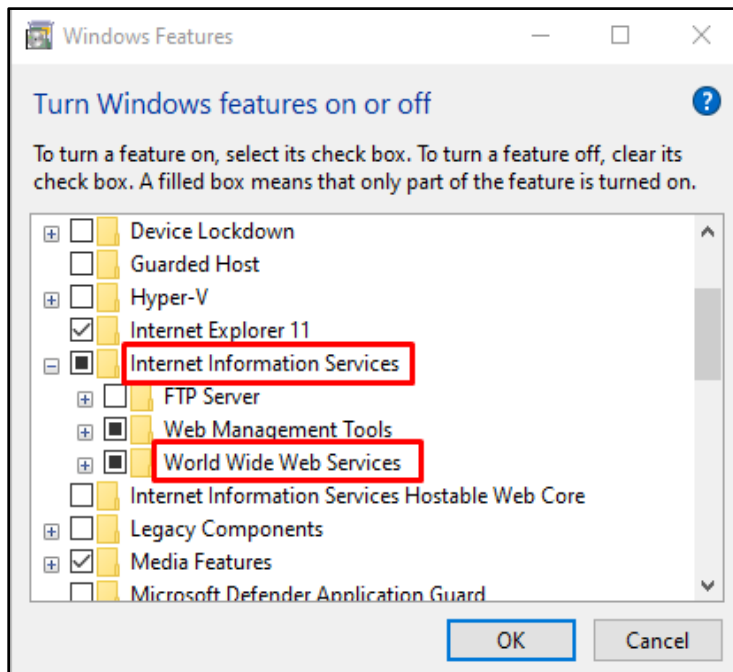1. Open **Control Panel** >> **Programs**.



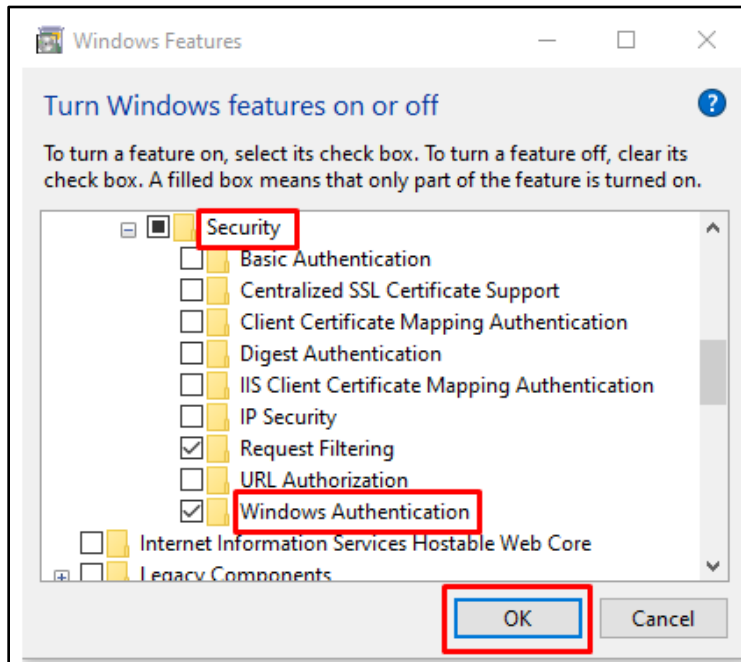2. Click on **Programs and Features.**

3. Click on **Turn Windows features on or off.**



4. Expand **Internet Information Services** >> **World Wide Web Services**.
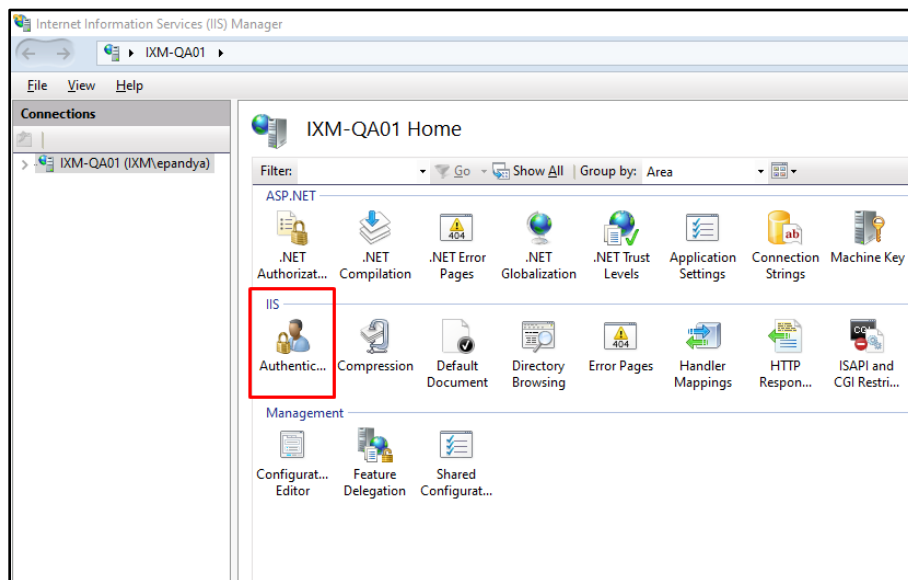
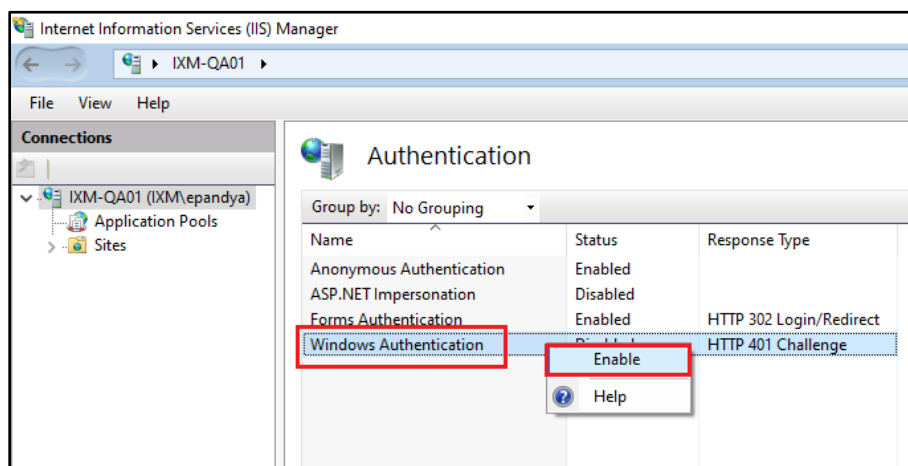5. Expand **Security** >> Enable **Windows Authentication.**



6. Click **OK** to finish the configuration.

## b) Enable Windows Authentication from IIS

1. Once IXM WEB is installed, open **IIS**.
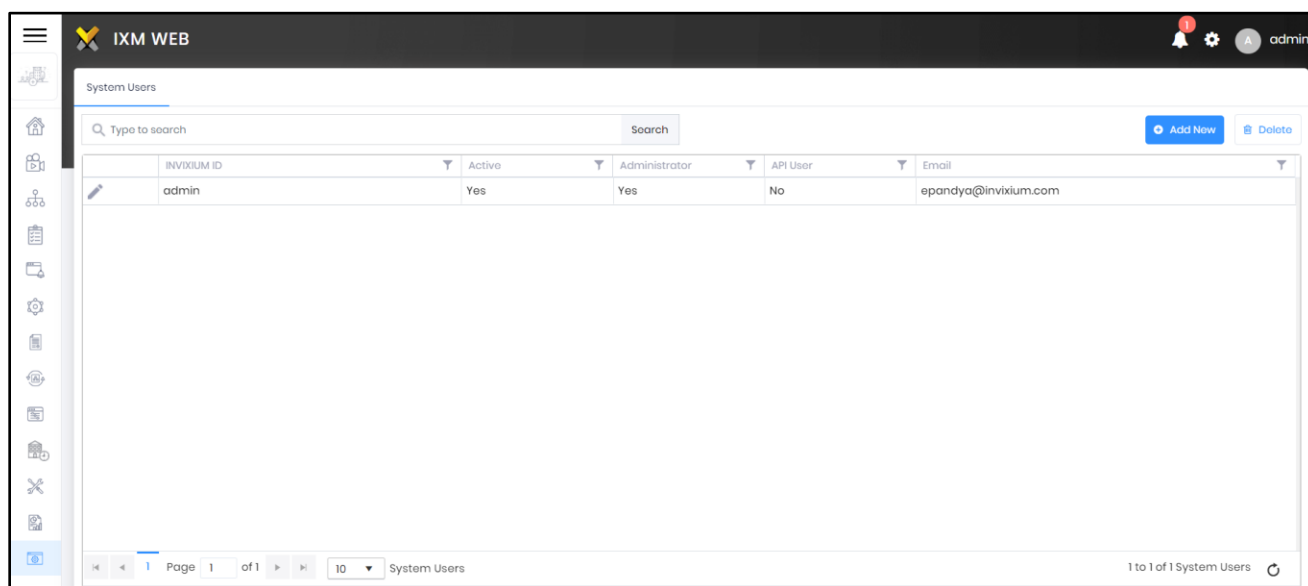2. Double click on **Authentication.**



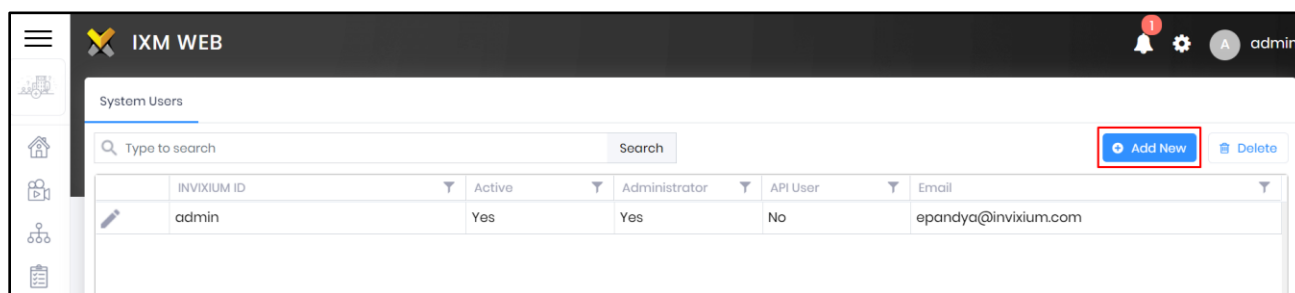3. Right click on **Windows Authentication** >> Click on **Enable**.

# Create System User(s) for SSO Login

**Note:** SSO login can only be enabled for domain users.

1. Log into IXM WEB.
2. On the home page, expand **Left Navigation Pane** >> **System**. The application will redirect to the System Users window.



3. Click on **Add New**.



4. Creating an SSO user requires the following details:
   - Login type: Domain employee
   - Invixium ID (User ID): For domain employee logins, User ID is automatically filled from AD
   - Password:  For domain employee logins, password creation is not required

- Email address
- Status
- SSO Login: Enable SSO login
- Permission for modules: Assign permission for modules based on the requirement.



5. Click on **Save**.

# Login with an SSO System User

Access IXM WEB in browser >> Click on **SSO Login**.
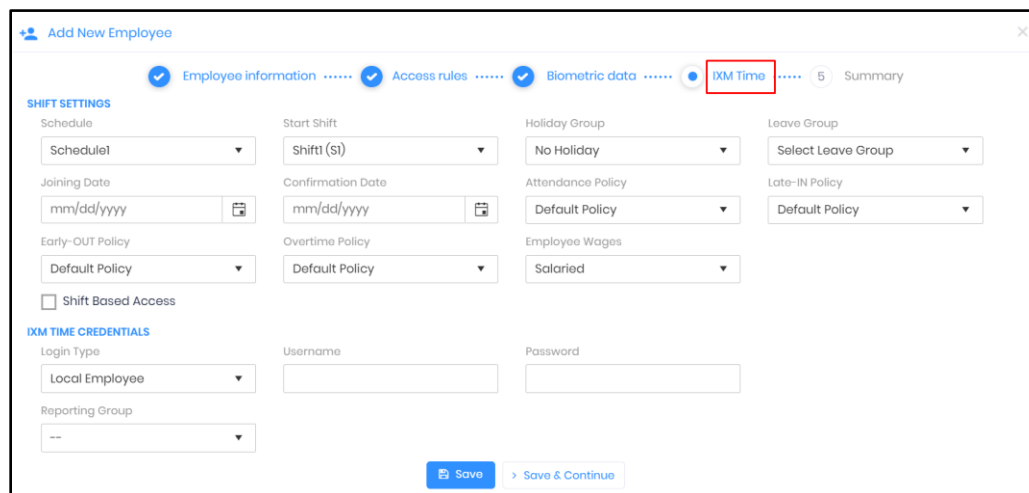
# Create IXM Time Employee(s) for SSO Login

**Note:** SSO login for IXM Time employees can only be enabled for domain users.

1. Once the IXM Time license is activated successfully, navigate to the **Employee** module >> Click on **Add Employee**.
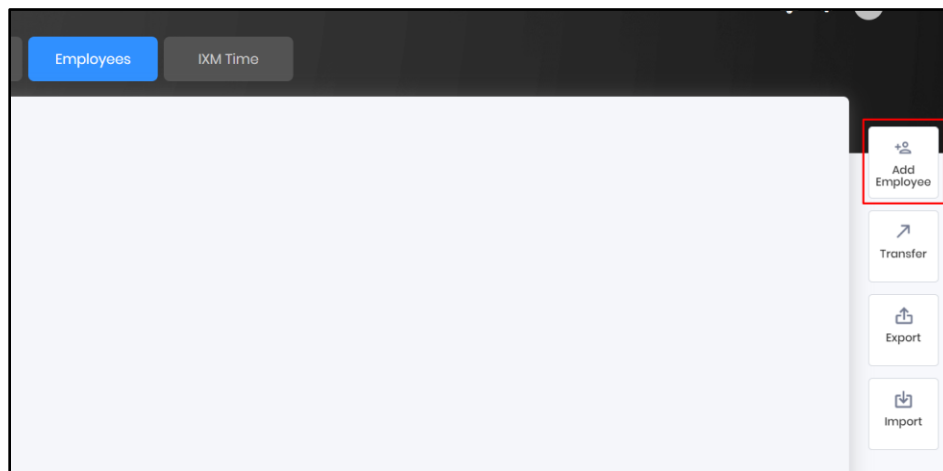


2. Enter employee details as per requirement >> Click on the **IXM Time** tab.



3. Creating an SSO user requires the following details:
   - Login type: Domain employee
   - Invixium ID (User ID): For domain employee logins, User ID is automatically filled from AD
   - Password:  For domain employee logins, password creation is not required

- SSO Login: Enable SSO login
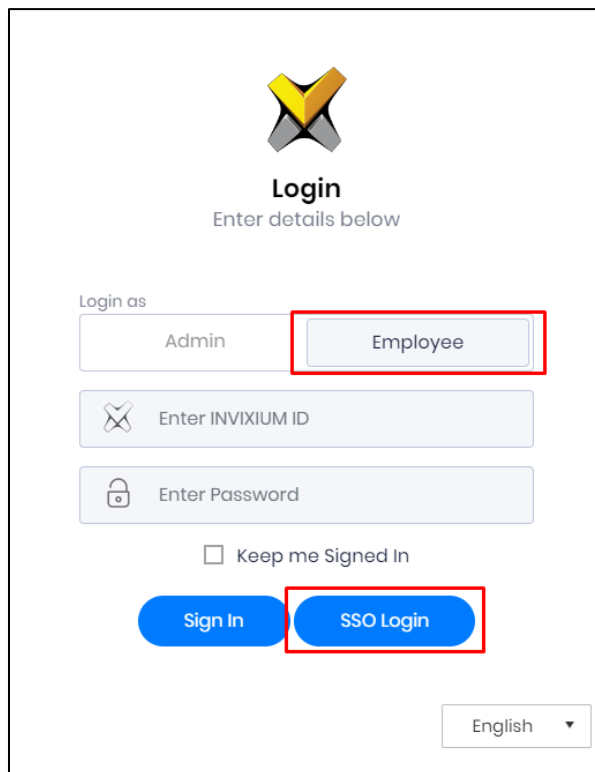


4. Click on **Save**.

# Login with an SSO IXM Time Employee

Access IXM WEB in browser >> Click on **Employee** tab >> Click on **SSO Login**.

# Configuring Default Login

## a) Configure Default Login to True

1. Go to the "**Invixium**" path in the machine where IXM WEB is installed.
2. Navigate to **IXM Web** >> Open web.config file**.**
3. Open **web.config** file in any text editor >> Search for "**DefaultLogin**" >>Update "**value**" to "**true**".

```
146     <add key="lenel_on_guard_bulk_page_number" value="0" />
147     <add key="lenel_on_guard_initial_import_mode" value="Incremental" />
148     <add key="lenel_on_guard_Time_diff" value="0" />
149     <add key="max_records" value="100" />
150     <add key="pro-watch_open_timeout_mins" value="10" />
151     <add key="pro-watch_close_timeout_mins" value="10" />
152     <add key="pro-watch_send_timeout_mins" value="60" />
153     <add key="pro-watch_receive_timeout_mins" value="60" />
154     <add key="pro-watch_initial_import_mode" value="Incremental" />
155     <add key="FireAlarmAPI" value="IXMWebApi/TransactionLog/GenerateFireAlarm" />
156     <add key="VisiorDocumentFiletePath" value="/VisitorDocuments/" />
157     <add key="NedapEnrollmentUrl" value="Link/EnrollNedapAEOSUser/" />
158     <add key="gallagher_pos_override" value="0" />
159     <add key="gallagher_initial_import_mode" value="Incremental" />
160     <add key="IXMMobile_Android_URL" value="https://play.google.com/store/apps/details?id=com.invixium.vitals" />
161     <add key="IXMMobile_IOS_URL" value="https://apps.apple.com/app/id1580758087" />
162     <add key="DefaultLogin" value="true" />
163   </appSettings>
164   <!--
```

4. Save the "**web.config**" file.

**Note:** Perform a hard refresh (i.e., ctrl + F5) if IXM WEB is already open in any browser after updating the IXM WEB config file.

**Result:** IXM WEB's login page will be displayed when the IXM WEB URL is accessed in the browser.

## b) Configure Default Login to False

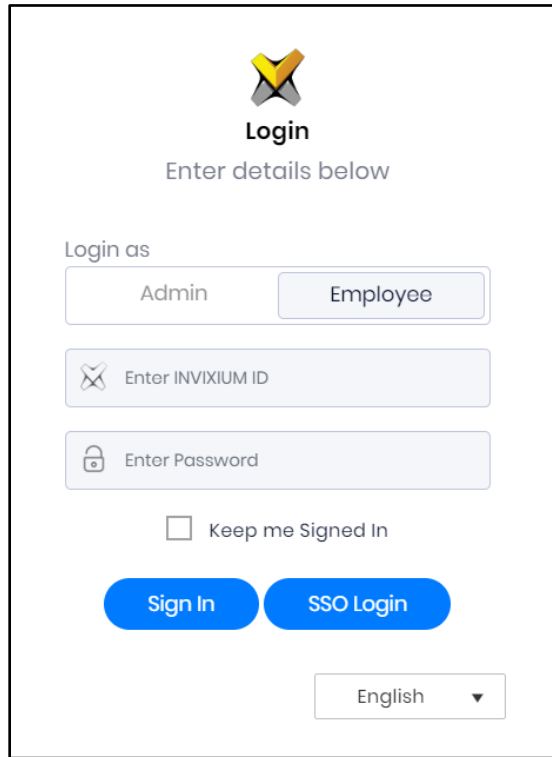1. Go to the "**Invixium**" path in the machine where IXM WEB is installed.
2. Navigate to **IXM Web** >> Open web.config file.
3. Open **web.config** file in any text editor >> Search for "**DefaultLogin**" >>Update "**value**" to "**false**".

```
143    <add key="genetec_max_degree_of_parallelism" value="50" />
144    <add key="lenel_og_max_degree_of_parallelism" value="5" />
145    <add key="pro-watch_bulk_page_number" value="0" />
146    <add key="lenel_on_guard_bulk_page_number" value="0" />
147    <add key="lenel_on_guard_initial_import_mode" value="Incremental" />
148    <add key="lenel_on_guard_Time_diff" value="0" />
149    <add key="max_records" value="100" />
150    <add key="pro-watch_open_timeout_mins" value="10" />
151    <add key="pro-watch_close_timeout_mins" value="10" />
152    <add key="pro-watch_send_timeout_mins" value="60" />
153    <add key="pro-watch_receive_timeout_mins" value="60" />
154    <add key="pro-watch_initial_import_mode" value="Incremental" />
155    <add key="FireAlarmAPI" value="IXMWebApi/TransactionLog/GenerateFireAlarm" />
156    <add key="VisiorDocumentFiletePath" value="/VisitorDocuments/" />
157    <add key="NedapEnrollmentUrl" value="Link/EnrollNedapAEOSUser/" />
158    <add key="gallagher_pos_override" value="0" />
159    <add key="gallagher_initial_import_mode" value="Incremental" />
160    <add key="IXMMobile_Android_URL" value="https://play.google.com/store/apps/details?id=com.invixium.vitals" />
161    <add key="IXMMobile_IOS_URL" value="https://apps.apple.com/app/id1580758087" />
162    <add key="DefaultLogin" value="false" />
163  </appSettings>
```

4. Save the "**web.config**" file.

**Note:** Perform a hard refresh (i.e., ctrl + F5) if IXM WEB is already open in any browser after updating the IXM WEB config file.

**Result:**

- SSO system users will directly login to IXM WEB when the IXM WEB URL is accessed in the browser.
- T&A SSO employees will directly login to the employee portal when the IXM WEB URL is accessed in the browser.

# FAQs

1. **Is SSO supported in Internet Explorer?**
   No, SSO is not supported in Internet Explorer.


2. **Is SSO supported in incognito mode?**
   No, SSO is not supported in incognito mode.


3. **When will the SSO login button appear on the login page?**
   SSO Login will only appear if at least 1 domain user is present in IXM WEB.


4. **Is SSO supported in Mozilla Firefox?**
   Yes, but clicking on the SSO Login button in the browser may askyour username and password in a  pop-up. In such cases, directly click on the sign-in button without entering your username and password.


5. **What if browsers do not trust the IXM WEB site for Windows authentication?**
   In such cases, end-users can use a self-signed certificate or can add the WEB URL under Local intranet from the control panel's Internet Options.

# Support

For more information relating to this Feature Description document, please contact us at support@invixium.com

# Disclaimers and Restrictions

This document and the information described throughout are provided in their present condition and are delivered without written, expressed, or implied commitments by Invixium Inc. and are subject to change without notice. The information and technical data herein are prohibited for the intention of reverse engineering and shall not be disclosed to parties for procurement or manufacturing.

This document may contain unintentional typos or inaccuracies.

TRADEMARKS

The trademarks specified throughout the document are registered trademarks of Invixium Inc. All third-party trademarks referenced herein are recognized to be trademarks of their respective holders or manufacturers.