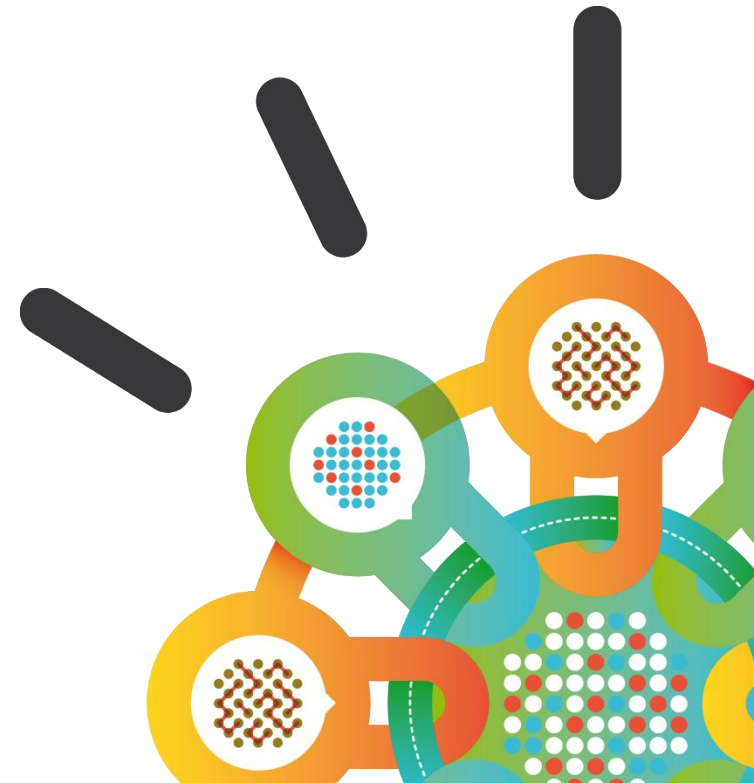


Security Intelligence.
Think Integrated.



MSS VSOC Portal Single Sign-On Using IBM id



Changes to VSOC Portal Sign In Page

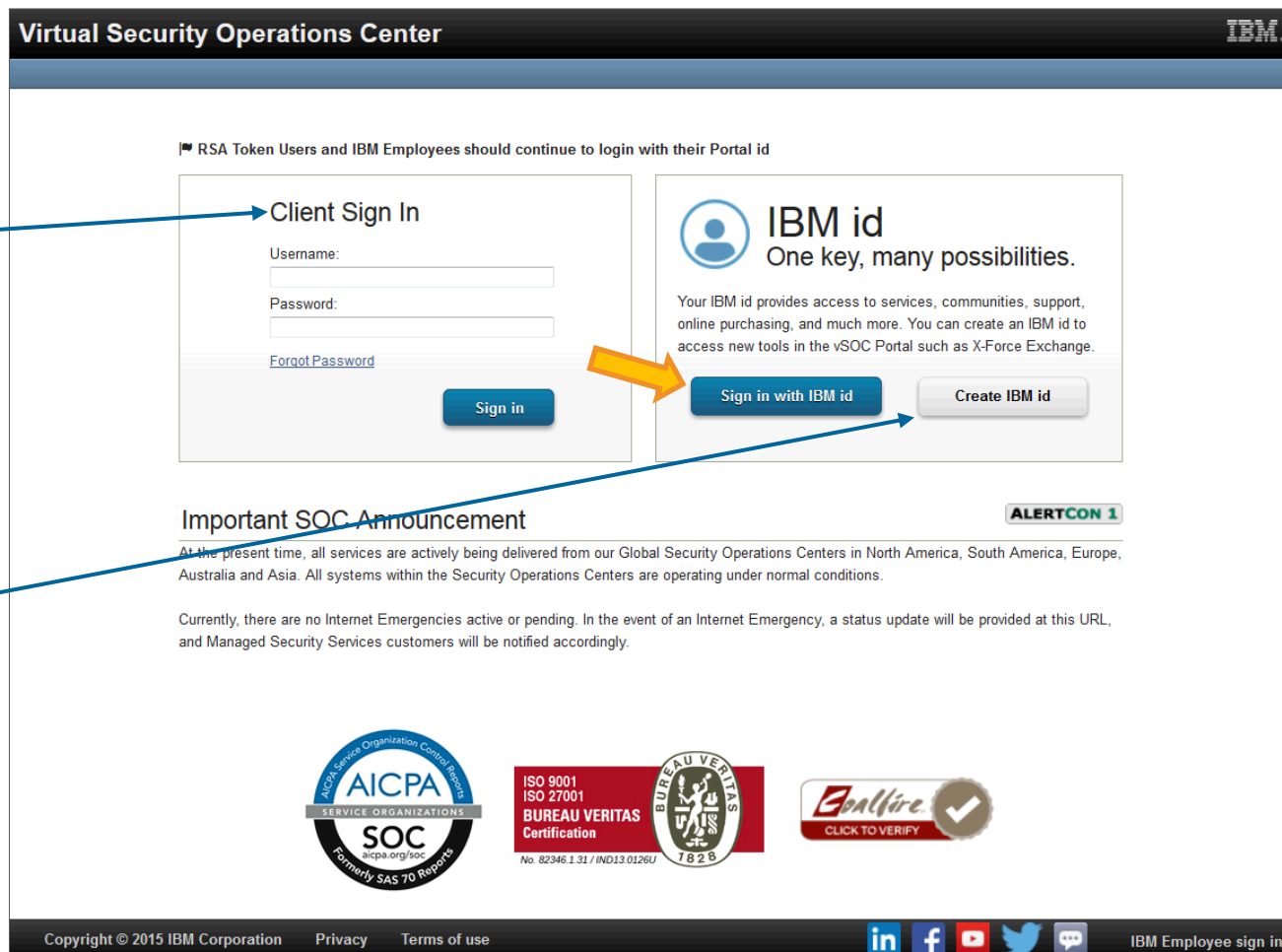
Notable Information

- Users can continue to use the existing Client Sign In on the left and enter their existing Portal username and password.

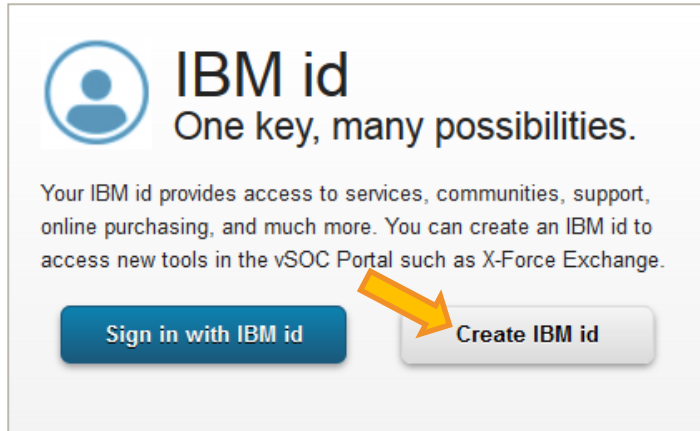
Note: Using IBM id is optional at this time.

- Users can select **Create IBM id**, if they don't already have one. Users will be taken to the IBM id registration page.

Note: IBM employees and users with RSA Tokens are not able to use IBM id for Portal at this time.



IBM id Registration Page (Use if you don't already have an IBM id)



IBM id
One key, many possibilities.

Your IBM id provides access to services, communities, support, online purchasing, and much more. You can create an IBM id to access new tools in the vSOC Portal such as X-Force Exchange.

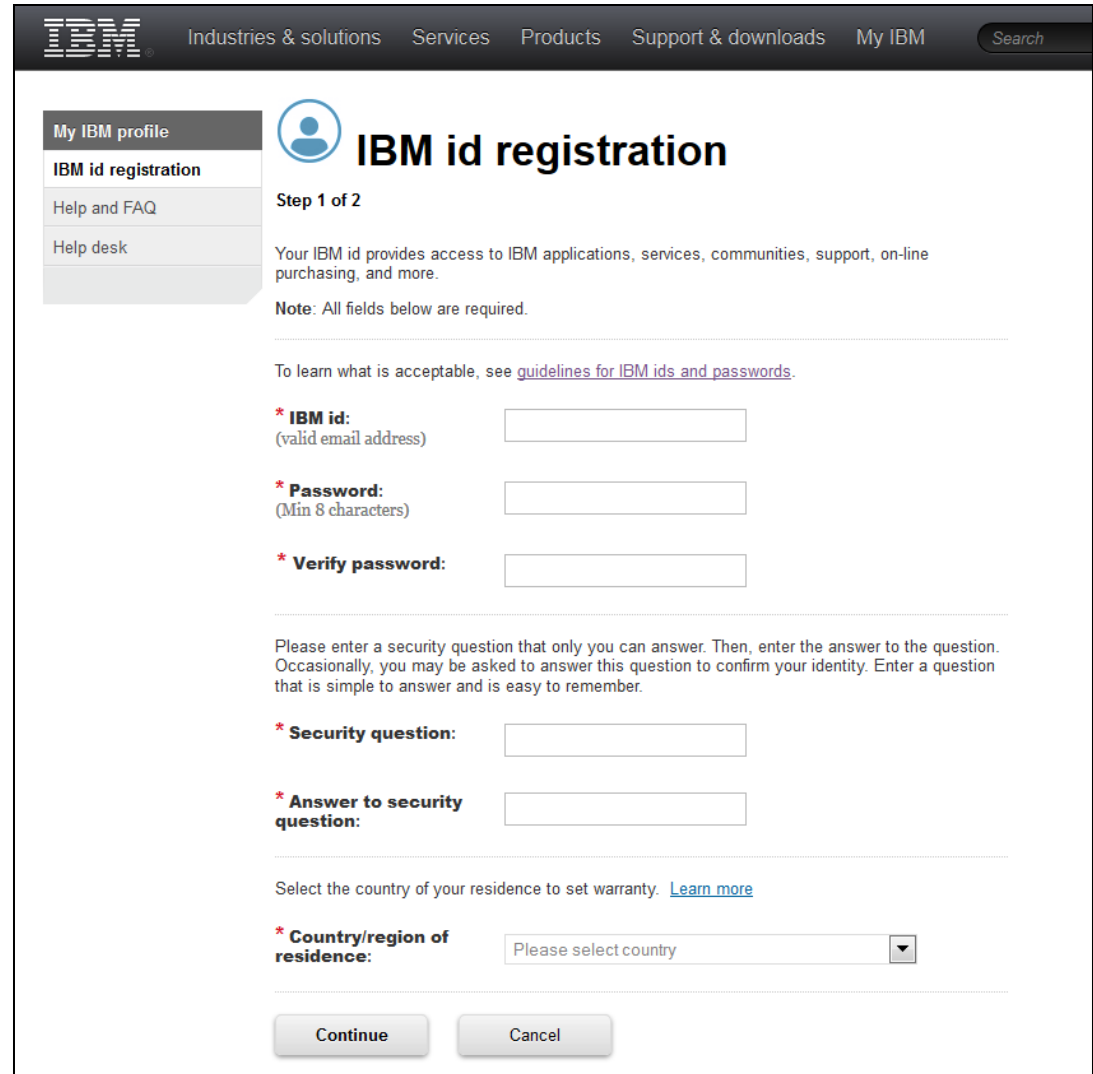
[Sign in with IBM id](#) [Create IBM id](#)

Notable Information

- Users can complete the registration pages and submit.

Note: This is a one-time setup step.

- The IBM id registration page is not managed by Managed Security Services, so we do not have the ability to change its content or appearance.



IBM Industries & solutions Services Products Support & downloads My IBM Search

My IBM profile

- IBM id registration
- Help and FAQ
- Help desk

IBM id registration

Step 1 of 2

Your IBM id provides access to IBM applications, services, communities, support, on-line purchasing, and more.

Note: All fields below are required.

To learn what is acceptable, see [guidelines for IBM ids and passwords](#).

* **IBM id:** (valid email address)

* **Password:** (Min 8 characters)

* **Verify password:**

Please enter a security question that only you can answer. Then, enter the answer to the question. Occasionally, you may be asked to answer this question to confirm your identity. Enter a question that is simple to answer and is easy to remember.

* **Security question:**

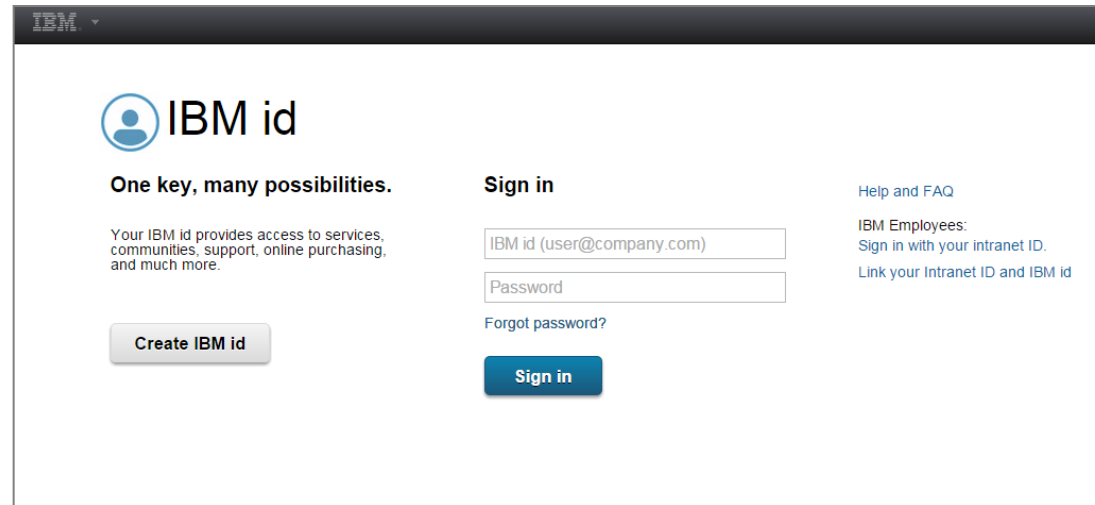
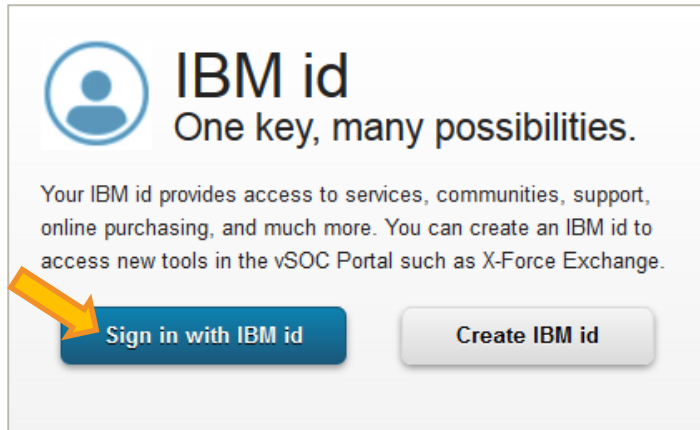
* **Answer to security question:**

Select the country of your residence to set warranty. [Learn more](#)

* **Country/region of residence:**

[Continue](#) [Cancel](#)

IBM id Sign In Page (Can be used with an existing IBM id)



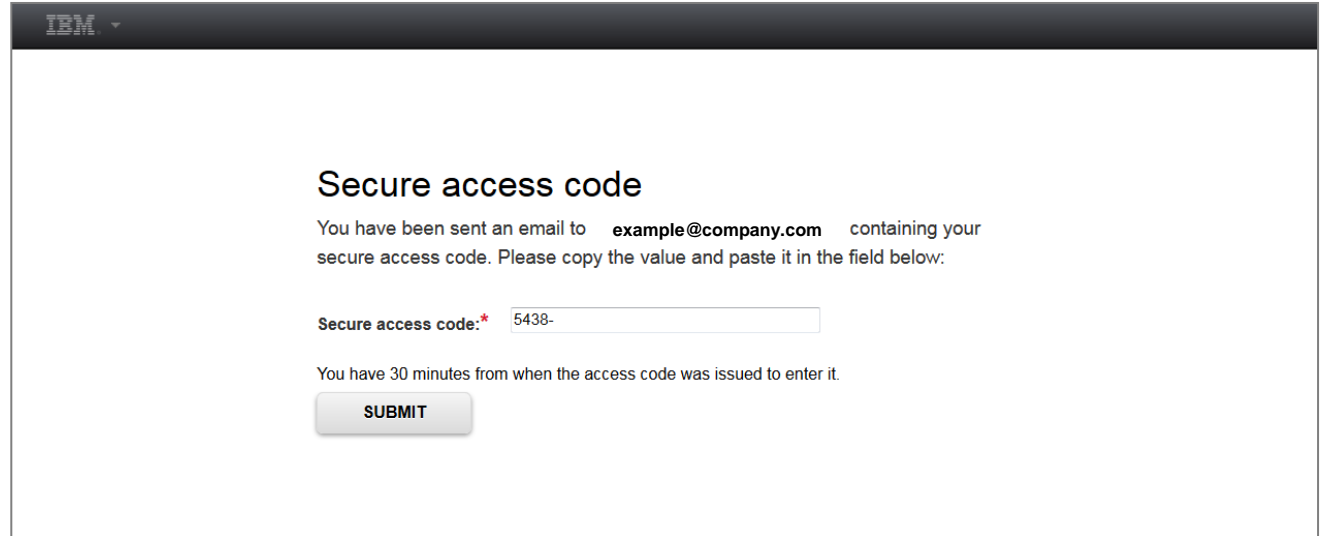
Notable Information

- Users can sign in with their existing IBM id.
- The IBM id Sign in page is not managed by Managed Security Services, so we do not have the ability to change its content or appearance.
- Upon successful sign in, users will receive an email with an access code from no-reply@IBM.com with the subject "IBM Bluemix Single Sign-On Service Security Access Code."

Verify email address to activate IBM id and intent to link accounts

Notable Information

- Users will have to enter the **Secure access code** included in the email and select **Submit**.
- The Secure access code page is not managed by Managed Security Services, so we do not have the ability to change its content or appearance.



The screenshot shows a web page with a dark header containing the IBM logo. The main content area is white and contains the following text and form elements:

Secure access code

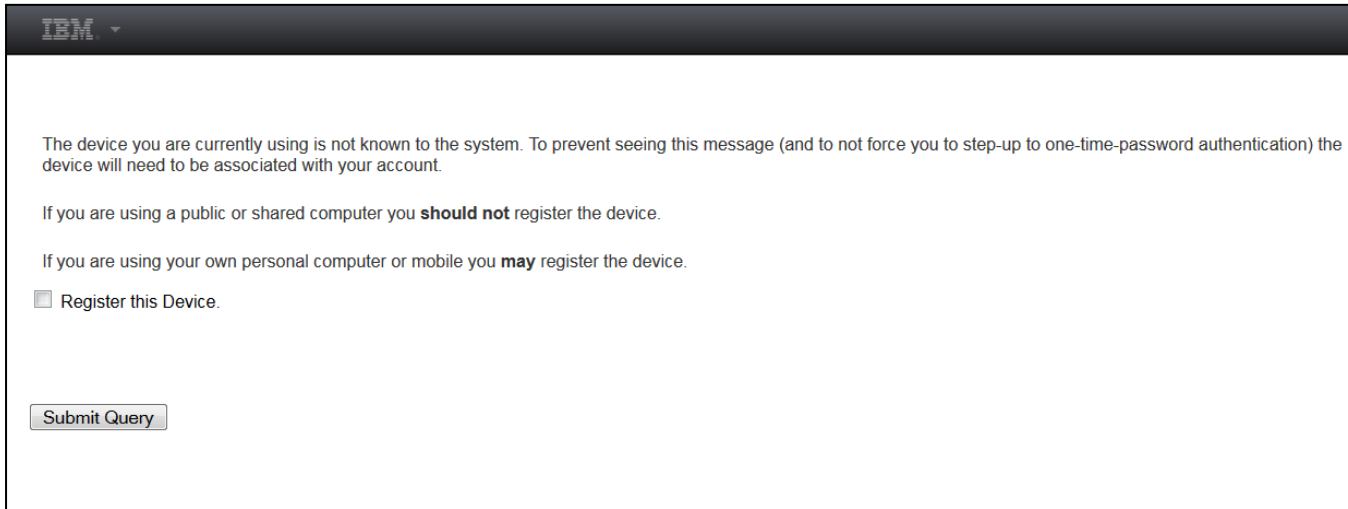
You have been sent an email to **example@company.com** containing your secure access code. Please copy the value and paste it in the field below:

Secure access code:*

You have 30 minutes from when the access code was issued to enter it.

SUBMIT

Registering Devices to use with IBM id



The screenshot shows a web page with the IBM logo in the top left corner. The main content area contains the following text:

The device you are currently using is not known to the system. To prevent seeing this message (and to not force you to step-up to one-time-password authentication) the device will need to be associated with your account.

If you are using a public or shared computer you **should not** register the device.

If you are using your own personal computer or mobile you **may** register the device.

Register this Device.

Submit Query

Notable Information

- Users will need to register each device they use to access applications using IBM id.
- Users are prompted to Register the Device to prevent the ongoing need to use the Secure Access code in the prior step.
- Users can choose to register the device and proceed by checking the **Register this Device** box and selecting **Submit Query**, or
- Users can choose not to register the device and proceed by leaving the **Register this Device** box unchecked and selecting **Submit Query**.
- This page is not managed by Managed Security Services, so we do not have the ability to change its content or appearance.

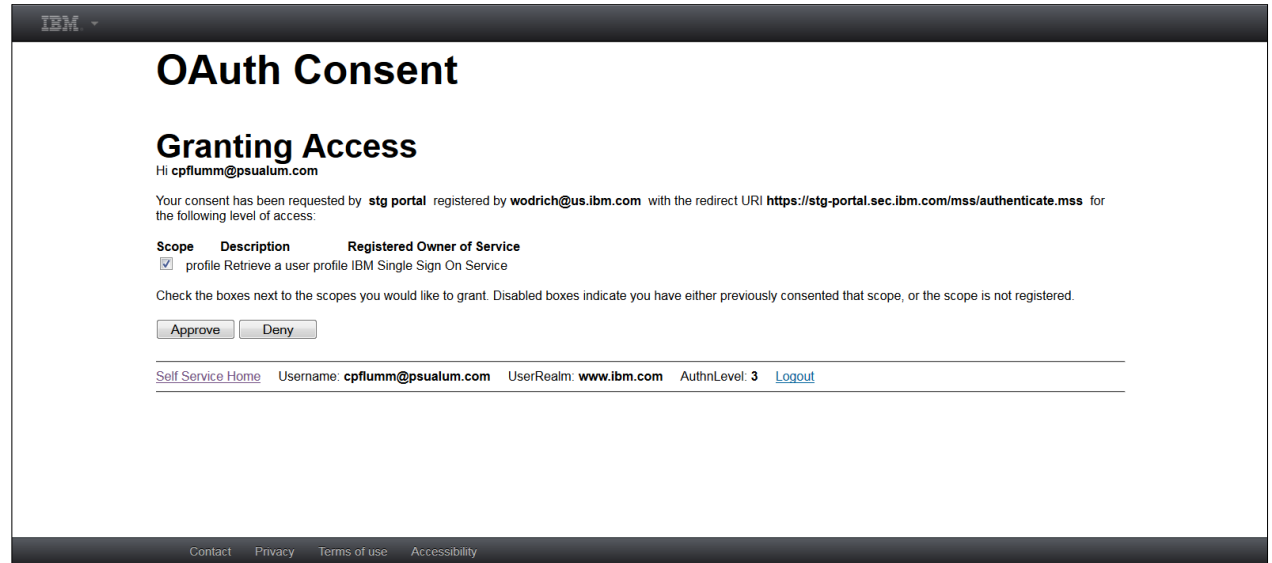
IBM id Consent

Notable Information

- Users may be prompted to consent to granting access to IBM id.

Notes:

- If you were granted access previously while using another IBM application, you might not receive this screen.
- This is a one-time setup step.
- The OAuth Consent page is not managed by Managed Security Services, so we do not have the ability to change its content or appearance.



The screenshot shows the IBM OAuth Consent page. At the top, it says "OAuth Consent" and "Granting Access". Below that, it says "Hi cpflumm@psualum.com". The main text reads: "Your consent has been requested by stg portal registered by wodrich@us.ibm.com with the redirect URI https://stg-portal.sec.ibm.com/mss/authenticate.mss for the following level of access:". There is a table with columns "Scope", "Description", and "Registered Owner of Service". The table contains one row: "profile Retrieve a user profile IBM Single Sign On Service". Below the table, it says "Check the boxes next to the scopes you would like to grant. Disabled boxes indicate you have either previously consented that scope, or the scope is not registered." There are two buttons: "Approve" and "Deny". At the bottom, there is a footer with links: "Self Service Home", "Username: cpflumm@psualum.com", "UserRealm: www.ibm.com", "AuthnLevel: 3", and "Logout".

VSOC Portal Account Linking Page

Notable Information

- Users are then redirected from the IBM id page back to the VSOC Portal.
- This page informs users they are now logged in with IBM id, though to use their IBM id with the VSOC Portal, they will need to link their account.

Note: After you link your account, the IBM id and password will replace your Portal id and password. Going forward, you will need to select **Sign in with IBM id** on the Portal Sign In page.


- After entering the existing Portal username and Password, and selecting **Link accounts and sign in**, users will be logged in to the VSOC Portal.

Virtual Security Operations Center
IBM.

Linking your IBM id to your vSOC Portal account

- ✔ You are logged in with your IBM id: cpflumm@psualum.com
- ! To gain access to vSOC Portal using your IBM id, link your vSOC Portal account.
- ! After you link your accounts, your IBM id will replace your Portal id.

Next time you log into the vSOC portal, you will need to click the 'Sign in with IBM id' button.



IBM id
One key, many possibilities.

Your IBM id provides access to services, communities, support, online purchasing, and much more. You will need to create an IBM id to access new tools in the vSOC Portal such as X-Force Exchange.

➔

Sign in with IBM id
Create IBM id

Link your IBM id by entering your vSOC portal credentials below:

Client Sign In

Username:

Password:

Link accounts and sign in

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY

Thank You

www.ibm.com/security



© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.