



# Mastering the STS Universal User with IBM<sup>®</sup> Security Access Manager

IBM SECURITY SUPPORT OPEN MIC



**NOTICE:** BY PARTICIPATING IN THIS CALL, YOU GIVE YOUR IRREVOCABLE CONSENT TO IBM TO RECORD ANY STATEMENTS THAT YOU MAY MAKE DURING THE CALL, AS WELL AS TO IBM'S USE OF SUCH RECORDING IN ANY AND ALL MEDIA, INCLUDING FOR VIDEO POSTINGS ON YOUTUBE. IF YOU OBJECT, PLEASE DO NOT CONNECT TO THIS CALL.



April 25, 2019

# Announcing IBM VIP Rewards

Engage. Earn points. Get Rewards.



IBM VIP Rewards is a way to engage with and recognize the ways that you, the client, add value to IBM. Complete fun challenges and get rewarded for interacting with IBM, learning new technologies and sharing your knowledge.

Learn more...  
[ibm.biz/vip-rewards](https://ibm.biz/vip-rewards)

Join IBM VIP Rewards for Security...  
[ibm.biz/JoinIBMVIPRewards-Security](https://ibm.biz/JoinIBMVIPRewards-Security)

**IBM**



IBM VIP Rewards for **Security**

# Come to IBM Security Master Skills University – May 13 - 17

*Location: Hilton Orlando Bonnet Creek – Orlando, FL*

- Learn more about your IBM Security product through advanced education sessions and hands on labs taught by the experts who build, deploy and support these products every day
- Network among a classroom of your peers that have a shared vision and passion for security
- Connect with support experts, discuss how you use your product, and share what you want to achieve with it in 2019

*7 tracks will run concurrently. All registrants must select one track in order to attend.*

- IBM QRadar - Basic
- IBM QRadar - Advanced
- IBM BigFix
- IBM Guardium
- IBM Resilient
- IBM Identity Governance & Intelligence (IGI)
- IBM Security Access Manager (ISAM) and Cloud Identity

**Register now: [ibm.com/events/2019/OrlandoMS](https://ibm.com/events/2019/OrlandoMS)**

**Conference fee: \$595 USD**



# IBM Security Learning Academy

[www.SecurityLearningAcademy.com](http://www.SecurityLearningAcademy.com)

New content  
published daily!



Learning at  
no cost!

Learning Videos ● Hands-on Labs ● Live Events

# Panelists

## Presenters

Annelise Quap – ISAM Level 2 Support Engineer

Gabriel Bell – ISAM Level 2 Support Engineer

Jack Yarborough – ISAM Level 2 Support Engineer

## Moderator

Kathy Hansen – ISAM Level 2 Support Manager

# Goal of Session

- Through this session one will understand how to find, format, and understand the contents of the STS Universal User (STSUU) XML Format for use during Advanced Access Control (AAC) and Federation flows.
- An ISAM Administrator should be able to successfully utilize Federation/AAC tracing to enhance their mapping rules and provide desired Identity Mapping for Single Sign-On

# Agenda

- STSUU Overview
- STSUU Format
- STSUU Contents during Common AAC Flows
- STSUU Contents during Common SSO Flows
- Parsing Techniques for the STSUU
- Linking the STSUU elements to the Java Methods
- Development Techniques for enhancing the STSUU
- Tracing Techniques for the STSUU



# STSUU Overview



# STSUU Overview

The STS Universal User (STSUU) is...

“an intermediate document in a generic XML format that holds identity information.”

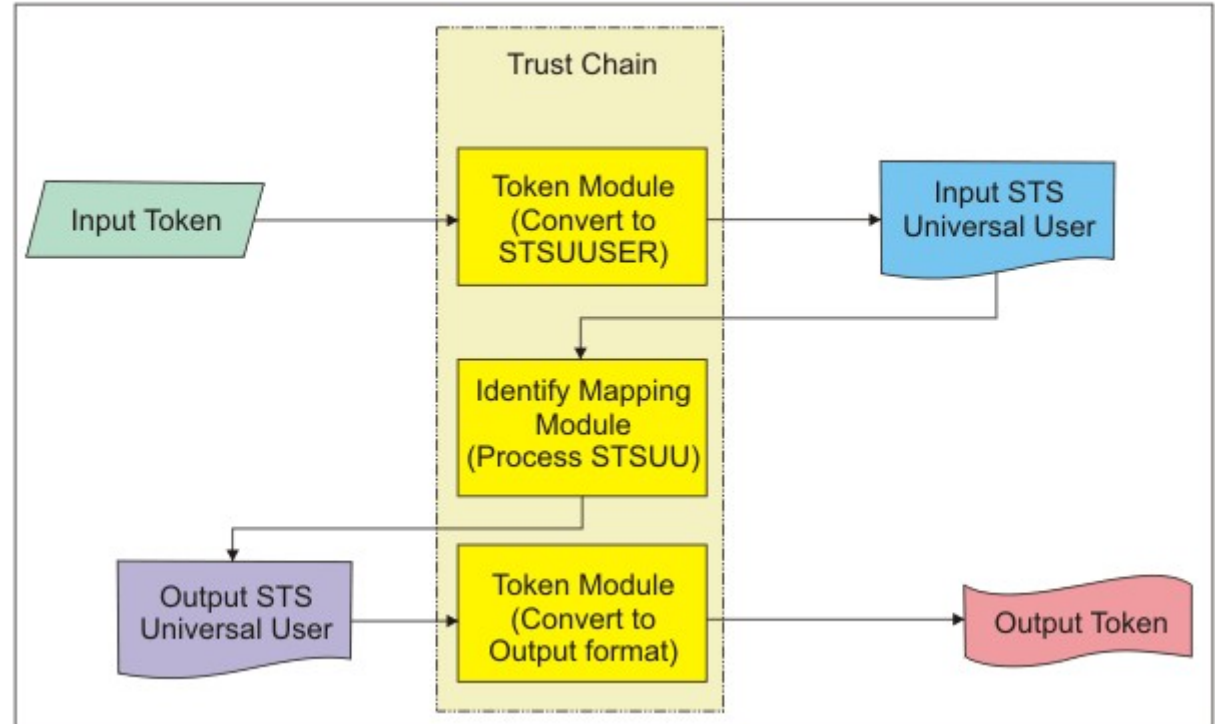
Ref - IBM Knowledge Center :  
ISAM 9.0.6.0 : **Security Token Service Universal User document**

But what does this mean?

This means you only have to know the STSUU format to map :

- SAML Tokens
- OIDC JWT and '/userinfo' response data
- OAUTH 2.0 Response Data

Figure 3. Token processing



Ref :

[https://www.ibm.com/support/knowledgecenter/en/SSZSXU\\_6.2.2.7/com.ibm.tivoli.fim.doc\\_6227/config/concept/federationidentitymappingSAML.html](https://www.ibm.com/support/knowledgecenter/en/SSZSXU_6.2.2.7/com.ibm.tivoli.fim.doc_6227/config/concept/federationidentitymappingSAML.html)



# STSUU Format



# Where can I find the STSUU Format?

The STSUU Schema is documented in the Knowledge Center!

ISAM Knowledge Center Reference:

[https://www.ibm.com/support/knowledgecenter/en/SSPREK\\_9.0.6/com.ibm.isam.doc/config/concept/stsuu\\_schema.html](https://www.ibm.com/support/knowledgecenter/en/SSPREK_9.0.6/com.ibm.isam.doc/config/concept/stsuu_schema.html)

TFIM Knowledge Center Reference:

[https://www.ibm.com/support/knowledgecenter/en/SSZSXU\\_6.2.2.7/com.ibm.tivoli.fim.doc\\_6227/config/concept/federationidentitymappingSAML.html](https://www.ibm.com/support/knowledgecenter/en/SSZSXU_6.2.2.7/com.ibm.tivoli.fim.doc_6227/config/concept/federationidentitymappingSAML.html)

# Parts of the STSUU – Identity Mapping

The STSUU contains four major parts that can be used for Identity Mapping:

- **Principal Information**
  - In the Access Manager environment this is information related to the current user
    - Username
    - UUID (used in ACLs)
    - LDAP DN
    - Access Manager Domain
- **Group Information**
  - In the Access Manager environment this is information related to the user's groups
    - Group name
    - Group DN
    - Group UUID (used in ACLs)
- **Attribute Information**
  - In the Access Manager environment this is information related to the user's Credential Attributes
- **Context Attribute Information**
  - In the Access Manger environment this is information related to the context of the request, mainly for OAUTH and OpenID flows

# Parts of the STSUU – Principal

The following is the STSUU Principal for the 'sec\_master' user during a SAML 2.0 flow:

```
<stsuser:Principal>  
  <stsuser:Attribute name="name" type="urn:ibm:names:ITFIM:5.1:accessmanager">  
    <stsuser:Value>sec_master</stsuser:Value>  
  </stsuser:Attribute>  
  <stsuser:Attribute name="uuid" type="urn:ibm:names:ITFIM:5.1:accessmanager">  
    <stsuser:Value>8de01a10-e86c-11e8-8616-00155de02155</stsuser:Value>  
  </stsuser:Attribute>  
  <stsuser:Attribute name="registryid" type="urn:ibm:names:ITFIM:5.1:accessmanager">  
    <stsuser:Value>cn=SecurityMaster,secAuthority=Default</stsuser:Value>  
  </stsuser:Attribute>  
  <stsuser:Attribute name="domain" type="urn:ibm:names:ITFIM:5.1:accessmanager">  
    <stsuser:Value>Default</stsuser:Value>  
  </stsuser:Attribute>  
</stsuser:Principal>
```

Container:Attribute:Value

Find me in your 'iv-user'!

Find me in your LDAP!

# Parts of the STSUU – GroupList

The following is a subset of the STSUU GroupList for the 'sec\_master' user during a SAML 2.0 flow:

```
<stsuser:GroupList>
  <stsuser:Group name="SecurityGroup" type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuser:Attribute name="uuid" type="urn:ibm:names:ITFIM:5.1:accessmanager">
      <stsuser:Value>8db37c94-e86c-11e8-8616-00155de02155</stsuser:Value>
    </stsuser:Attribute>
    <stsuser:Attribute name="registryid" type="urn:ibm:names:ITFIM:5.1:accessmanager">
      <stsuser:Value>cn=SecurityGroup,secAuthority=Default</stsuser:Value>
    </stsuser:Attribute>
  </stsuser:Group>
  <stsuser:Group name="ivmgrd-servers" type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuser:Attribute name="uuid" type="urn:ibm:names:ITFIM:5.1:accessmanager">
      <stsuser:Value>8e14b70c-e86c-11e8-8616-00155de02155</stsuser:Value>
    </stsuser:Attribute>
    <stsuser:Attribute name="registryid" type="urn:ibm:names:ITFIM:5.1:accessmanager">
      <stsuser:Value>cn=ivmgrd-servers,cn=SecurityGroups,secAuthority=Default</stsuser:Value>
    </stsuser:Attribute>
  </stsuser:Group>
  ...
</stsuser:GroupList>
```

Find me in the 'iv-groups' header!

Find me in your LDAP Server!

# Parts of the STSUU – AttributeList

The following is an excerpt of the STSUU AttributeList for the 'sec\_master' user during a SAML 2.0 flow:

```
<stsuuser:AttributeList>
  <stsuuser:Attribute name="AZN_CRED_AUTH_METHOD" type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuuser:Value>password</stsuuser:Value>
  </stsuuser:Attribute>
  ...
  <stsuuser:Attribute name="AZN_CRED_NETWORK_ADDRESS_STR" type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuuser:Value>10.2.0.1</stsuuser:Value>
  </stsuuser:Attribute>
  <stsuuser:Attribute name="AZN_CRED_AUTHNMECH_INFO" type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuuser:Value>LDAP Registry</stsuuser:Value>
  </stsuuser:Attribute>
  ...
  <stsuuser:Attribute name="tagvalue_max_concurrent_web_sessions" type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuuser:Value>unlimited</stsuuser:Value>
  </stsuuser:Attribute>
  <stsuuser:Attribute name="tagvalue_login_user_name" type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuuser:Value>sec_master</stsuuser:Value>
  </stsuuser:Attribute>
  <stsuuser:Attribute name="emailAddress" type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuuser:Value>sec_master@hyperv.lab</stsuuser:Value>
  </stsuuser:Attribute>
</stsuuser:AttributeList>
```

Add me in the Reverse Proxy Configuration File with [TAM\_CRED\_ATTRS\_SVC:eperson]  
Provided by the Reverse Proxy by default

# Parts of the STSUU – ContextAttributeList

The following is an excerpt of the STSUU ContextAttributeList for the 'sec\_master' user during an OAUTH Authorization Code Flow, before the 'PreTokenGeneration' Mapping Rule:

```
<stsuuser:ContextAttributes>
  <stsuuser:Attribute name="client_id" type="urn:ibm:names:ITFIM:oauth:query:param">
    <stsuuser:Value>3vDN0MMjTorJlwtabZ1L</stsuuser:Value>
  </stsuuser:Attribute>
  <stsuuser:Attribute name="request_type" type="urn:ibm:names:ITFIM:oauth:request">
    <stsuuser:Value>authorization</stsuuser:Value>
  </stsuuser:Attribute>
  <stsuuser:Attribute name="response_type" type="urn:ibm:names:ITFIM:oauth:query:param">
    <stsuuser:Value>code</stsuuser:Value>
  </stsuuser:Attribute>
  <stsuuser:Attribute name="username" type="urn:ibm:names:ITFIM:oauth:request">
    <stsuuser:Value>sec_master</stsuuser:Value>
  </stsuuser:Attribute>
  <stsuuser:Attribute name="redirect_uri" type="urn:ibm:names:ITFIM:oauth:query:param">
    <stsuuser:Value>https://isam9060.hyperv.lab/favicon.ico</stsuuser:Value>
  </stsuuser:Attribute>
  <stsuuser:Attribute name="definition_name" type="urn:ibm:names:ITFIM:oauth:request">
    <stsuuser:Value>azncode</stsuuser:Value>
  </stsuuser:Attribute>
</stsuuser:ContextAttributes>
```

Provided via User Input

Inserted by AAC



# STSUU Contents during Common AAC Flows



# OAUTH 2.0 Authorize Flow – Context Attributes

## Authorization Code using Query Arguments – '/authorize' endpoint

URL used to initiate :

[https://isam9060.hyperv.lab/apisvc/sps/oauth/oauth20/authorize?client\\_id=azncode\\_client&redirect\\_uri=https://isam9060.hyperv.lab/favicon.ico&scope=email&response\\_type=code](https://isam9060.hyperv.lab/apisvc/sps/oauth/oauth20/authorize?client_id=azncode_client&redirect_uri=https://isam9060.hyperv.lab/favicon.ico&scope=email&response_type=code)

```
<stsuser:ContextAttributes>
  <stsuser:Attribute name="client_id" type="urn:ibm:names:ITFIM:oauth:query:param">
    <stsuser:Value>azncode_client</stsuser:Value>
  </stsuser:Attribute>
  <stsuser:Attribute name="scope" type="urn:ibm:names:ITFIM:oauth:query:param">
    <stsuser:Value>email</stsuser:Value>
  </stsuser:Attribute>
  ...
  <stsuser:Attribute name="response_type" type="urn:ibm:names:ITFIM:oauth:query:param">
    <stsuser:Value>code</stsuser:Value>
  </stsuser:Attribute>
  ...
  <stsuser:Attribute name="redirect_uri" type="urn:ibm:names:ITFIM:oauth:query:param">
    <stsuser:Value>https://isam9060.hyperv.lab/favicon.ico</stsuser:Value>
  </stsuser:Attribute>
</stsuser:ContextAttributes>
```

# OAuth 2.0 /token endpoint – Context Attributes

Authorization Code using Query Arguments – '/token' endpoint – Before Mapping

```
Request made : curl -k "https://isam9060.hyperv.lab/apisvc/sps/oauth/oauth20/token" --data-ascii  
"client_id=azncode_client&grant_type=authorization_code&redirect_uri=https://isam9060.hyperv.lab/favicon.ico&code=JgPdFiN3Y75xELbJcf0shJ80fny8RJ"
```

```
<stsuser:ContextAttributes>  
  <stsuser:Attribute name="redirect_uri" type="urn:ibm:names:ITFIM:oauth:body:param">  
    <stsuser:Value>https://isam9060.hyperv.lab/favicon.ico</stsuser:Value>  
  </stsuser:Attribute>  
  ...  
  <stsuser:Attribute name="code" type="urn:ibm:names:ITFIM:oauth:body:param">  
    <stsuser:Value>JgPdFiN3Y75xELbJcf0shJ80fny8RJ</stsuser:Value>  
  </stsuser:Attribute>  
  <stsuser:Attribute name="grant_type" type="urn:ibm:names:ITFIM:oauth:body:param">  
    <stsuser:Value>authorization_code</stsuser:Value>  
  </stsuser:Attribute>  
  <stsuser:Attribute name="client_id" type="urn:ibm:names:ITFIM:oauth:body:param">  
    <stsuser:Value>azncode_client</stsuser:Value>  
  </stsuser:Attribute>  
</stsuser:ContextAttributes>
```

# AAC MFA Flow - EULA

The AAC 'Authentication Service' will run the 'authsvc\_credential.js' mapping rule after an Authentication Policy or mechanism has been performed. The following is an example of 'juser' after he has submitted his EULA. It has been abbreviated for readability:

```
<?xml version="1.0" encoding="UTF-8"?>
<stsuser:STSUniversalUser xmlns:stsuser="urn:ibm:names:ITFIM:1.0:stsuser">
  <stsuser:Principal>
    <stsuser:Attribute name="name">
      <stsuser:Value>juser</stsuser:Value>
    </stsuser:Attribute>
  </stsuser:Principal>
  <stsuser:AttributeList>
...
    <stsuser:Attribute name="AUTHENTICATION_LEVEL">
      <stsuser:Value>1</stsuser:Value>
    </stsuser:Attribute>
...
    <stsuser:Attribute name="authenticationTransactionId">
      <stsuser:Value>4270073a-b57e-4453-82cd-31a09da8f28a</stsuser:Value>
    </stsuser:Attribute>
...
    <stsuser:Attribute name="authenticationTypes">
      <stsuser:Value>urn:ibm:security:authentication:asf:eula</stsuser:Value>
    </stsuser:Attribute>
...
  </stsuser:AttributeList>
  <stsuser:RequestSecurityToken/>
  <stsuser:ContextAttributes/>
  <stsuser:AdditionalAttributeStatement/>
</stsuser:STSUniversalUser>
```



# STSUU Contents during Common SSO Flows



# SAML 2.0 – Request Security Token Claims Data

This excerpt is from a SAML 2.0 Service Provider Flow

```
<stsuser:Attribute name="Claims" type="com:tivoli:am:fim:sts:RST">
  <stsuser:Value>
    <wst:Claims xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust" Dialect="urn:ibm:names:ITFIM:saml">
      <fimc:SamI20Claims xmlns:fimc="urn:ibm:names:ITFIM:saml">
        AssertionConsumerServiceURL=https://isam9060.hyperv.lab/svc/sps/services/saml20/login
        DefaultNameIDFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
        ProtocolProfile="urn:oasis:names:tc:SAML:2.0:profiles:SSO"
        RelayState="https%3A%2F%2Fisam9060.hyperv.lab%2Fpics%2Fiv30.gif"
        SignatureValidated="true"
        Target="https%3A%2F%2Fisam9060.hyperv.lab%2Fpics%2Fiv30.gif"/>
      </fimc:SamI20Claims>
    </wst:Claims>
  </stsuser:Value>
</stsuser:Attribute>
```



# Parsing Techniques for the STSUU



# Parsing Techniques – External Tools

## Applications:

- Notepad++ 'XML Tools' Plugin (Windows)
  - Ctrl + Alt + Shift + B -- XML Pretty Print with Indentions
- Sublime Text (Mac)
  - Selection -> Format -> Indent XML
    - This is available after installing the 'Indent' plugin

## Command Line Methods:

- XmlLint.exe (Cygwin)
  - `xmlLint.exe --pretty 1 stsuu.xml -o stsuu_formatted.xml`
- sed
  - `sed 's/></>\r\n</g' stsuu.xml > stsuu_formatted.xml`
- Perl and `cat`
  - `cat stsuu.xml | perl -e "s/></>\r\n</g" -p > stsuu_formatted.xml`

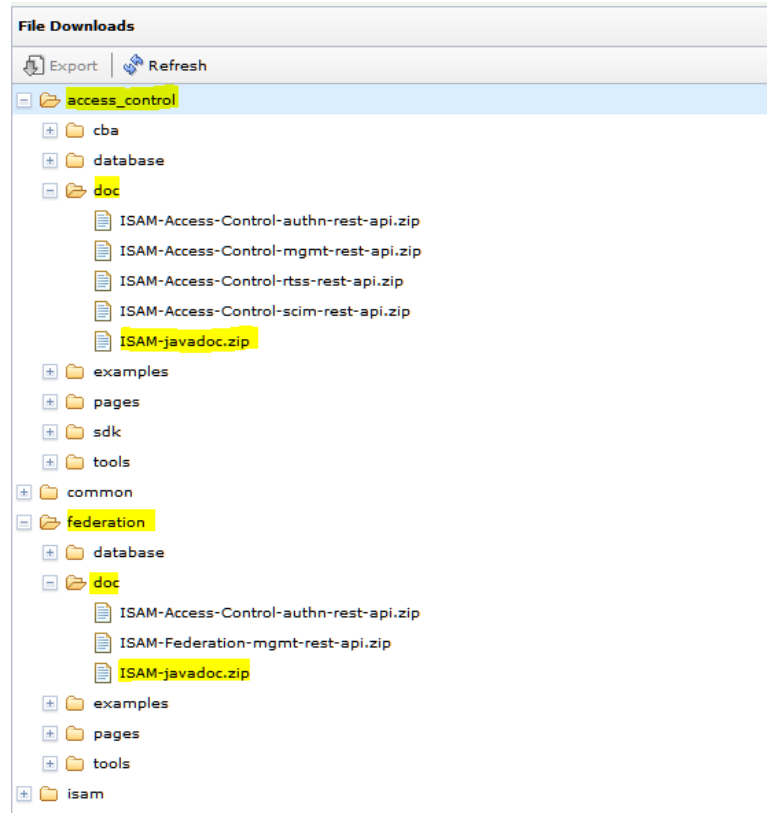
---

# Linking the STSUU elements to the Java Methods



# Location of the Java Documentation

Manage System Settings -> Secure Settings -> File Downloads



# Relevant Java Classes and Methods – The Principal Container

XML Representation of the Principal (IdP Federation) :

```
<stsuser:STSUniversalUser xmlns:stsuser="urn:ibm:names:ITFIM:1.0:stsuser">
  <stsuser:Principal>
    <stsuser:Attribute name="name" type="urn:ibm:names:ITFIM:5.1:accessmanager">
      <stsuser:Value>sec_master</stsuser:Value>
    </stsuser:Attribute>
  </stsuser:Principal>
  ...
</stsuser:STSUniversalUser>
```

Generic Reference For All Containers

Attribute Container

Attribute

Attribute Value

The java class used to access this data would be the 'STSUniversalUser' class in the 'com.tivoli.am.fim.trustserver.sts' Package

Common Methods for accessing contents :

getPrincipalAttributeContainer() - Returns an 'AttributeContainer' representation of the Principal Attribute Container

getPrincipalAttributes() – Returns a 'java.util.Iterator' representation of the Principal Attribute Container

getPrincipalAttributeValueByName(java.lang.String name) – Returns a 'java.lang.String' value of the Principal Attribute specified, if present

In this example, the following methods would yield :

- var principalAttributeContainer = stsuu.getPrincipalAttributeContainer();
  - The 'principalAttributeContainer' would be an 'AttributeContainer' object containing all the 'Principal Attributes'
- var principalAttributeIterator = stsuu.getPrincipalAttributes();
  - The 'principalAttributeIterator' would be an 'Iterator' object containing all the 'Principal Attributes'
- var principalAttributeValue = stsuu.getPrincipalAttributeValueByName("name");
  - The 'principalAttributeValue' would hold the value 'sec\_master' from the 'name' attribute

# Relevant Java Classes and Methods – Retrieving Attributes

Attributes can be acquired from each part of the STSUniversalUser document in three formats

- ‘AttributeContainer’
  - Package : com.tivoli.am.fim.trustserver.sts.uuser
  - Class : AttributeContainer
    - Has documented methods in the ‘ISAM-javadoc.zip’ included in the appliance
- ‘java.util.Iterator’
  - Package : java.util
  - Class : Iterator
    - <https://docs.oracle.com/javase/8/docs/api/java/util/Iterator.html>
- ‘java.lang.String’
  - Package : java.lang
  - Class : String
    - <https://docs.oracle.com/javase/8/docs/api/java/lang/String.html>

Example of directly retrieving an Attribute called ‘email’ from the Attribute Container :

```
var emailAttrValue = stsuu.getAttributeContainer().getAttributeValueByName("email");
```

This is the same as :

```
var attrContainer = stsuu.getAttributeContainer();  
var emailAttrValue = attrContainer.getAttributeValueByName("email");
```

# Relevant Java Classes and Methods – Clearing the STSUU Containers

Often you will want to restrict the attributes in the 'output token'. The following methods are available:

- Class 'STSUniversalUser'

- clear()
  - This clears the current full STSUniversalUser object - <stsuser:STSUniversalUser xmlns:stsuser="urn:ibm:names:ITFIM:1.0:stsuser">
- clearAttributeList()
  - This clears the 'AttributeList' - <stsuser:AttributeList>
- clearAttributeStatements()
  - This clears the 'AttributeStatement' - <stsuser:AdditionalAttributeStatement>
- clearContextAttributes()
  - This clears the 'ContextAttributes' - <stsuser:ContextAttributes>
- clearGroupList()
  - This clears the 'GroupList' - <stsuser:GroupList>
- clearPrincipal()
  - This clears the 'Principal' - <stsuser:Principal>
- clearRequestSecurityToken()
  - This clears the 'RequestSecurityToken' - <stsuser:RequestSecurityToken>

Clear Individual Attribute Containers like :

```
attributeContainerVar.clear()
```

Code Example :

```
# Save the initial attribute list  
var initialAttrContainer =  
stsuu.getAttributeContainer();
```

```
# Clear the initial attribute list  
stsuu.clearAttributeList();
```

# Relevant Java Classes and Methods – Removing Individual Attributes

You may want to remove specific attributes from the 'output token'. The following methods are available:

- Class 'STSUniversalUser'
  - removeAttribute(java.lang.String name, java.lang.String type)
    - This removes an attribute of the specified name and type from the stsuu
  - removeGroup(java.lang.String name, java.lang.String type)
    - This removes the specified group
  - removePrincipalAttribute(java.lang.String name, java.lang.String type)
    - This removes the specified principal attribute

Code Example :

```
# Remove a group named 'testgroup'  
stsuu.removeGroup("testgroup", "urn:ibm:names:ITFIM:5.1:accessmanager");
```

```
# Remove an attribute called email  
stsuu.removeAttribute("mail", "urn:ibm:names:ITFIM:5.1:accessmanager");
```

```
# Remove a context attribute called 'scope'  
stsuu.removeAttribute("scope", "urn:ibm:names:ITFIM:oauth:query:param");
```

```
# Remove a principal Attribute called 'uuid'  
stsuu.removePrincipalAttribute("uuid", "urn:ibm:names:ITFIM:5.1:accessmanager");
```

# Relevant Java Classes and Methods – Adding Attributes to the STSUU

Often you will want to add more attributes to the 'output token'. The following methods are available:

- Class 'STSUniversalUser'
  - addAttribute(Attribute attr)
    - This adds an attribute to the 'AttributeList' - <stsuuser:AttributeList>
  - addAttributeStatement(AttributeStatement attrstmt)
    - This adds an 'AttributeStatement' to the list of 'AttributeStatements' - <stsuuser:AdditionalAttributeStatement>
  - addContextAttribute(Attribute attr)
    - This adds an attribute to the 'ContextAttributes' - <stsuuser:ContextAttributes>
  - addGroup(Group group)
    - This adds a group to the 'GroupList' - <stsuuser:GroupList>
  - addPrincipalAttribute(Attribute attr)
    - This adds an attribute to the 'Principal' - <stsuuser:Principal>
  - The Request Security Token is 'read only'

Code Example :

# Adding an Attribute

```
stsuu.addAttribute(new Attribute("testattr","urn:ibm:names:ITFIM:5.1:accessmanager","testvalue"));
```

# Adding a Group

```
stsuu.addGroup(new Group("testgroup"));
```

# Adding a Context Attribute that will appear in the response (OAUTH /authorize or /token)

```
stsuu.addContextAttribute(new Attribute("test_rsp_attr","urn:ibm:names:ITFIM:oauth:response:attribute","testvalue"));
```



# Development Techniques for enhancing the STSUU



# Tips for Performance

- ❖ Use 'getAttributeByNameAndType(String name, String type)' when searching through the Context Attribute Container
- ❖ Declare commonly used attributes at the 'global scope' when possible
  - This allows all functions, logical statements, and loops to access the variables
    - Be aware of where else the variables are used!
  - This minimizes the memory footprint

# Good Coding Practices

- ❖ Break your code into container based logic
  - Gather Each container at the start of your mapping rule

```
var attrContainer = stsuu.getAttributeContainer();
var contextAttrContainer = stsuu.getContextAttributesAttributeContainer();
var reqSecurityTokenContainer = stsuu.getRequestSecurityTokenAttributeContainer();
var principalAttrContainer = stsuu.getPrincipalAttributeContainer();
var groupIterator = stsuu.getGroups();
var numGroups = stsuu.getNumberOfGroups();
```

- ❖ Check for null values before adding attributes to the stsuu

```
if(attr != null && attr.length() >0) {
    stsuu.addAttribute(attr);
}
```

// Remember to use comments

```
/* Even if they span
over multiple lines.
They help other people understand */
```



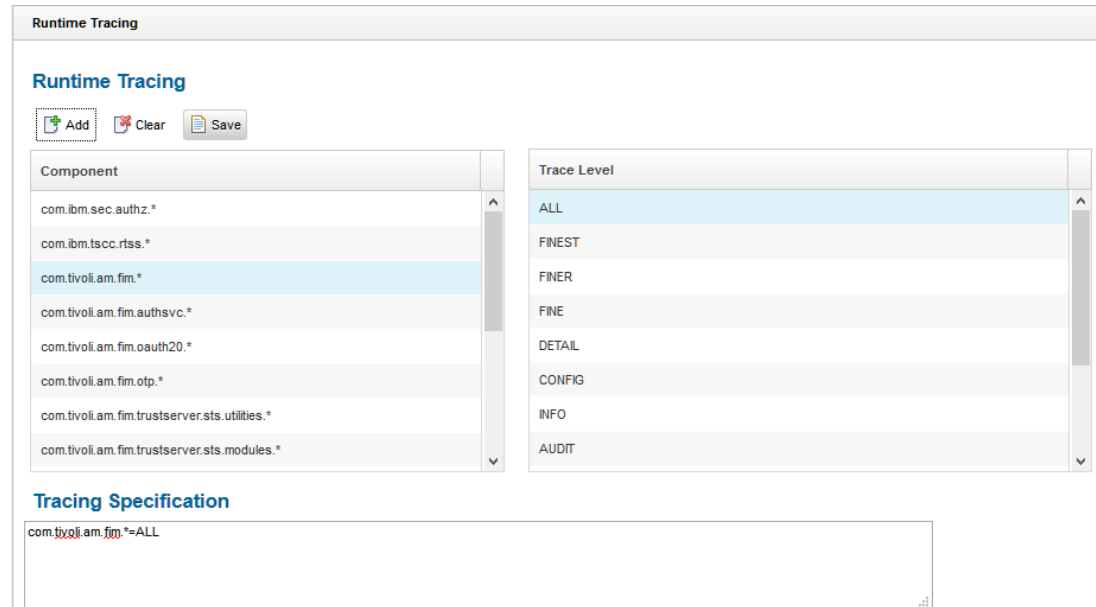
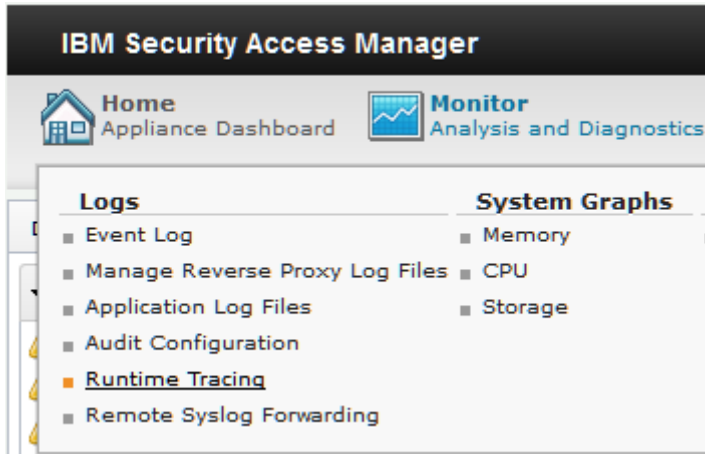
# Tracing Techniques for the STSUU



# Setting Tracing

Where do I set AAC/Federation Tracing?

'Monitor Analysis and Diagnostics -> Logs -> Runtime Tracing'

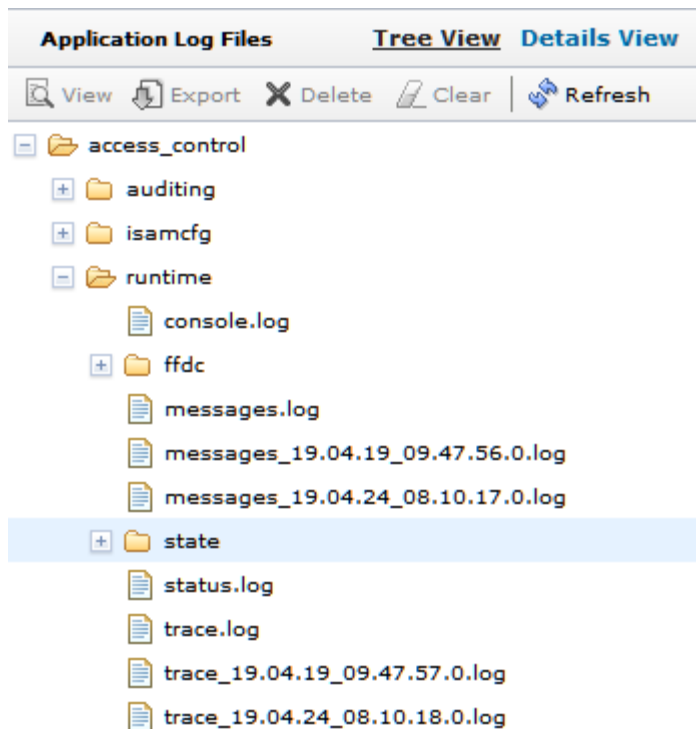


# Trace Log Locations

Where do I get the trace logs after I recreate an issue?

'Monitor Analysis and Diagnostics -> Logs -> Application Log Files'

From this menu you navigate to either 'access\_control' or 'federation' and then the subsequent 'runtime' folder



# Trace Specifications to get just the STSUU

What specifications can I set to get the STSUU at every point?

The following Specifications will get the STSUU for all transactions in each type of flow:

- Federation SSO Flow

- `com.tivoli.am.fim.trustserver.sts.modules.STSTokenIVCred=ALL:com.tivoli.am.fim.trustserver.sts.STSModuleChainManager=ALL:com.tivoli.am.fim.trustserver.sts.STSModuleChain=ALL`

- Access Control MFA Flow

- `com.tivoli.am.fim.authsvc.util.AuthSvcCredentialMappingRule=ALL`

- Access Control OAUTH 2.0 Flow

- `com.tivoli.am.fim.oauth20.protocol.delegates.OAuth20BaseAuthorizeDelegate=ALL:com.tivoli.am.fim.protocol.util.LocalTokenUtils=ALL:com.tivoli.am.fim.trustserver.sts.STSModuleChainManager=ALL:com.tivoli.am.fim.trustserver.sts.STSModuleChain=ALL:com.tivoli.am.fim.oauth20.mapping.OAuth20AppliancePreTokenMapModule=ALL:com.tivoli.am.fim.oauth20.strategy.commands.GetClientDefinitionCmd=ALL:com.tivoli.am.fim.trustserver.sts.modules.OAuth20TokenModule=ALL:com.tivoli.am.fim.oauth20.mapping.OAuth20AppliancePostTokenMapModule=ALL:com.tivoli.am.fim.oauth20.strategy.commands.ProduceOidcClaimsCmd=ALL`

# Questions for the panel

***Now is your opportunity to ask questions of our panelists.***

## **To ask a question now:**

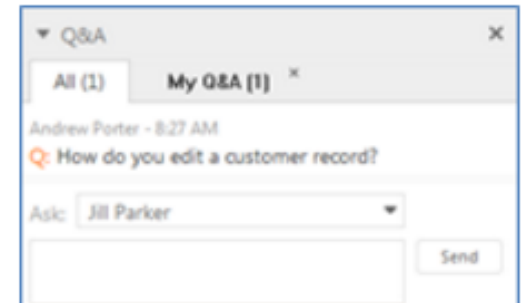
**Raise your hand by clicking Raise Hand.** The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.

or

**Type a question in the box below the Ask drop-down menu in the Q&A panel.**

**Select *All Panelists* from the Ask drop-down-menu.**

**Click Send.** Your message is sent and appears in the Q&A panel.



# Where do you get more information?

- **This slide presentation:** <http://www.ibm.com/support/docview.wss?uid=ibm10881007>
- **Security Learning Academy:** <https://ibm.biz/ISAM-LearningAcademy>
- **IBM Knowledge Center:** <https://www.ibm.com/support/knowledgecenter/en/SSPREK/welcome.html>
- **NEW ISAM Support forum:** <http://ibm.biz/ISAM-support-forum>

## Useful links:

[Get started with IBM Security Support](#)

[IBM My Support](#) | [Sign up for “My Notifications”](#)

[FREE learning resources on the Security Learning Academy](#)

[ibm.com/security/community](http://ibm.com/security/community)

## Follow us:



[www.youtube.com/user/IBMSecuritySupport](http://www.youtube.com/user/IBMSecuritySupport)



[twitter.com/askibmsecurity](http://twitter.com/askibmsecurity)



<http://ibm.biz/ISCS-LinkedIn>



# THANK YOU

## FOLLOW US ON:

 [youtube/user/IBMSecuritySupport](https://www.youtube.com/user/IBMSecuritySupport)

 [@askibmsecurity](https://twitter.com/askibmsecurity)

 [IBM Security Client Success](#)

 [SecurityLearningAcademy.com](https://www.ibm.com/security/learning-academy)

 [securityintelligence.com](https://www.ibm.com/security/intelligence)

 [xforce.ibmcloud.com](https://www.ibm.com/xforce)

 [ibm.com/security/community](https://www.ibm.com/security/community)

© Copyright IBM Corporation 2019. 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. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. 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.

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.