VDAB Security

VDAB provides different features

- Named users and user roles when using Android Client
- Optional whitelist access.
- Security Level Lockdown for web access.

Before This	You should have reviewed the Visual Dataflow Introduction tutorial or documentation.

Contents

Related Documentation

The following document and tutorials either are a) available or b) being developed to further support this subject.

Related Guides	Details

Related Tutorial	Details

VDAB User Roles

Users running the VDAB Android Client are associated with a specific user name which has been registered. If a user performs the initial configuration on a container, they will be added as an administrator on the Container or Server.

Additional users can be given privileges on the container by creating a role for them on that container.

Registered User Name

When an Android Client is registered, a user name is picked and registered.

User Roles

Individuals accessing VDAB using the Android Client will be mapped to one or more roles associated with the VDAB Server. The following roles the typical capabilities of each role:

Role	Actions Permitted
Observer	Observers can view flows, charts and properties. They can copy flows into their own server or container.
Operator	Operators can create flows, run flows and edit the properties of nodes and flows. They are not able change the container attributes or perform administrative actions.
Administrator	Administrators can change and any container property and perform any operations on a container. They are also able to assign roles to other Users.

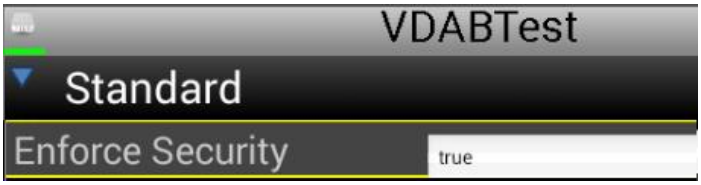
Enforcing Server Side Security

Warning	While security can be left disabled during initial testing, server side security should always be enabled when a system is considered in production.

Both the Android Client and the Server can restrict access based on the user role.

The role restrictions enforced by the Android Client, which makes certain menu actions unavailable, can't be disabled.

The role restrictions enforced on the server can be disabled or enabled by setting the Enforce Security property appropriately. This flag also enables or disables whitelist restrictions.

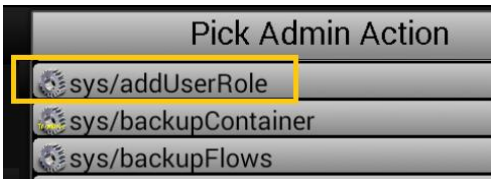


Adding Users with Roles

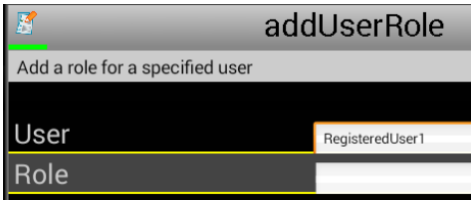
After the initial container is configured, additional users can be added by running addUserRole administrative tool.

1. While on the container main screen, click on the tools icon

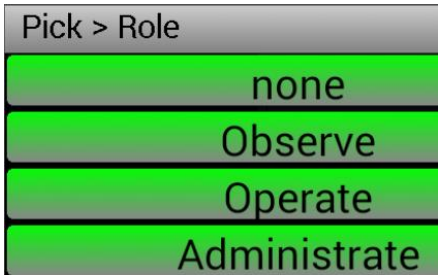
2. Click on the *addUserRole* Admin Action.



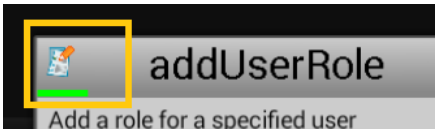
3. Enter the registered user



4. Double click on the role field and pick one of the available roles.

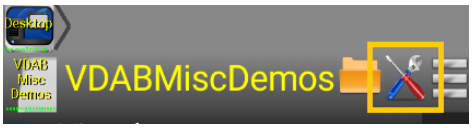


5. Click on the upper left to save the changes which will take effect immediately

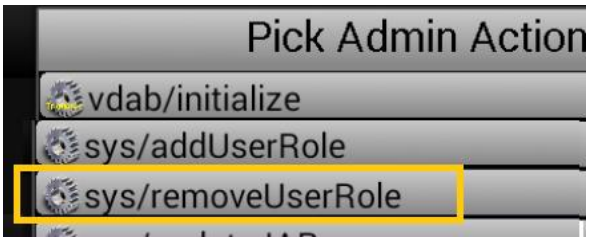


Removing User Roles

1. While on the container main screen, click on the tools icon

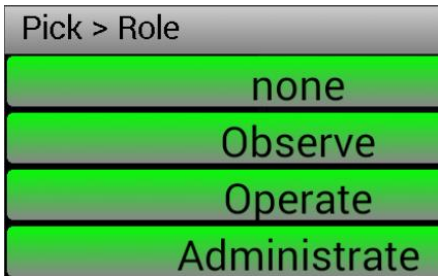


2. Click on the *removeUserRole* Admin Action.



3. Enter the registered user

4. Double click on the role field and pick one of the available roles.



5. Click on the upper left to save the changes which will take effect immediately

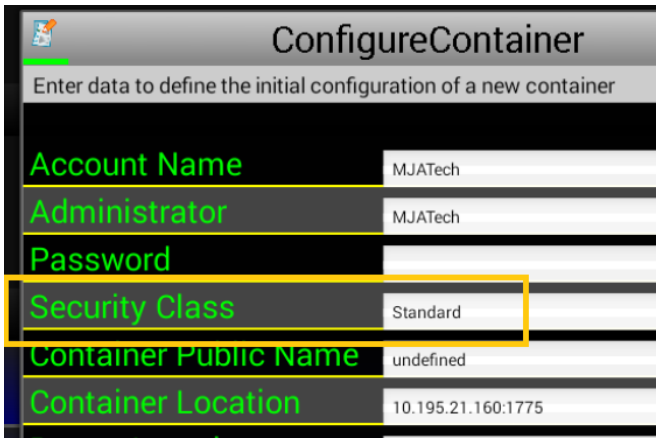
Editing User Roles in the container.xml

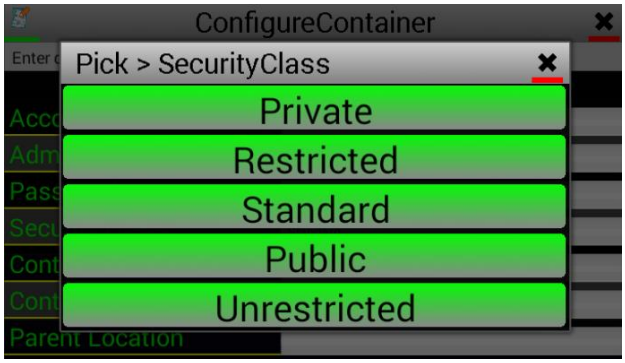
User role information is directly written to the container.xml file.

If desired user roles can be added or changed by directly edting this file.

Initial Security Class

When a container is initially configured, a container property called security class impacts how the initial security is configured. The property can also be edited later to reduce the access provided to individuals using the web client.





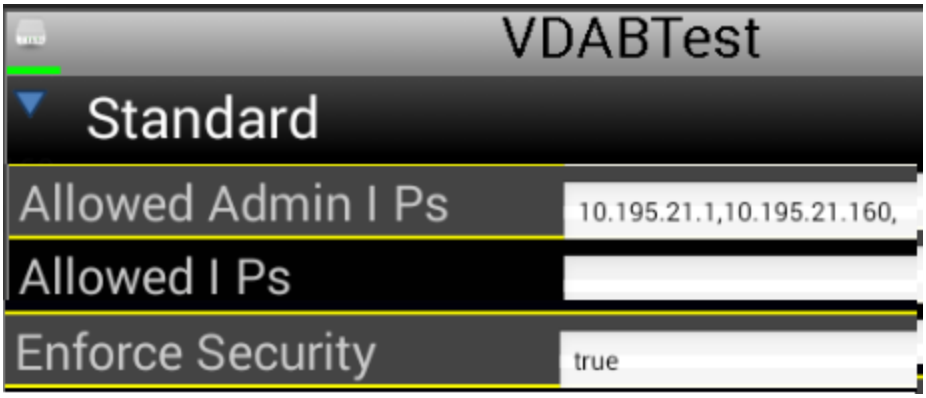
The impact on the initial role settings and web client access are detailed below:

Security Class	Rolese for Android Client Access	Web Client Access
Private	Observe – Initial Administrator Operate – Initial Administrator Administrate – Initial Administrator	No Web Access
Restricted	Observe – Known users. Operate – Initial Administrator Administrate – Initial Administrator	Anyone can observe
Standard	Observe – Any users. Operate – Initial Administrator Administrate – Initial Administrator	Anyone can observe
Public	Observe – Any users. Operate – Known Users Administrate – Initial Administrator	Anyone can operate and administer
Unrestricted	bserve – Any users. Operate – Known Users Administrate – Initial Administrator	Anyone can operate and administer

Whitelist Support

An additional level of security can be added by restricting which server addresses can access the VDAB Container. By default all IPs are allowed access. If any IP is specified in the whitelist the whitelist of allowed originating IPs will be used to restrict access to only those IPs

The following VDAB Container properties are associated with enabling and specifying whitelists:

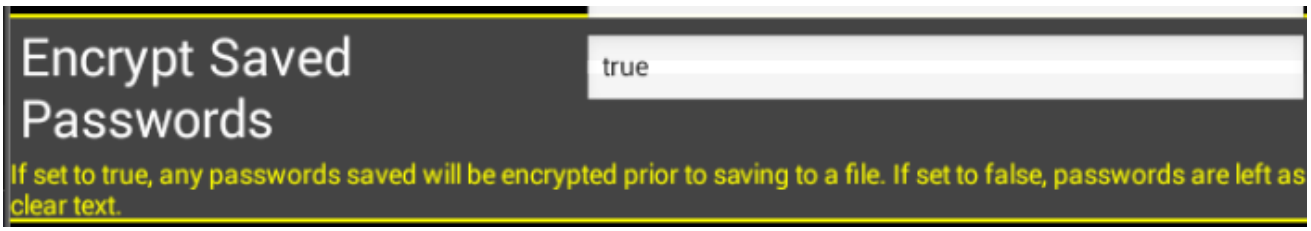


Container Attribute	Description
Allowed IPs	If set, restricts any access to the originating IPs specified in the comma delimited list. If left blank access is not restricted by IP. This makes the system inaccessible from other IPs and will restrict all access including pinging the server. Parent container must allow the IPs of children in order for them to send events and status.
Allowed Admin IPs	If set, restricts administrator access to the originating IPs specified in the comma delimited list. Someone If left blank access is not restricted by IP.
Enforce Security	If set to true, security will be enforced by the server.

If access to VDAB should be restricted to a limited number of originating addresses, a whitelist specified in the AllowedIPs or AllowedAdminIPs can be added.

Encryption for Passwords Used in Nodes and Forms

By default any password which is entered in a node will be encrypted when save to a configuration file. This behavior can be changed by editing the Encrypt Saved Passwords property for the container.



Password Encryption

Any field designated as a password type is 1) not display when entering data and 2) encrypted when saved to a configuration file.

Password can be directly entered in a flow or config file and will remain unencrypted until the flow or container configuration is save at which time they will be encrypted.

These encrypted passwords will only work on the container where they were originally entered. (If a flow with a password is copied to another container, the password will no longer work and it will need to be reentered.)

Designated Transferable Passwords

If you do want encrypted passwords to work after copying a flow from one container to another you must use a password that is designated as transferable.

Any password starting with a **!** will work when and will continue to work when the flow using the password is copied from one container to another.