Qlik Sense Security Rules List

Qlik Sense 3.2SR1

2017/03/03

Table of Contents

Read Only Security Rules

App

If you have read rights on the app you should be able to read app data segments belonging to that app

Name	Resource filter	Conditions	Context	Actions
ReadAppDataSegments	App.DataSegment_*	resource.App.HasPrivilege("read") and !user.IsAnonymous()	Both in hub and QMC	Read

If you have update rights on the app you should be able to create/update/read/delete app data segments belonging to that app

Name	Resource filter	Conditions	Context	Actions
UpdateAppDataSegments	App.DataSegment_*	resource.App.HasPrivilege("update") and !user.IsAnonymous()	Both in hub and QMC	Create Read Update Delete

If you have read rights on the app you should be able to read app internals belonging to that app

Name	Resource filter	Conditions	Context	Actions
ReadAppInternals	App.Internal_*	resource.App.HasPrivilege("read")	Both in hub and QMC	Read

If you have update rights on the app you should be able to create/update/read/delete app internals belonging to that app

Name	Resource filter	Conditions	Context	Actions
UpdateAppInternals	App.Internal_*	resource.App.HasPrivilege("update")	Both in hub and QMC	Create Read Update Delete

If you have read rights on the app you should be able to read app content belonging to that app

Name	Resource filter	Conditions	Context	Actions
ReadAppContents	App.Content_*	resource.App.HasPrivilege("read")	Both in hub and QMC	Read

If you have update rights on the app you should be able to update app content belonging to that app

Name	Resource filter	Conditions	Context	Actions
UpdateAppContents	App.Content_*	resource.App.HasPrivilege("update")	Both in hub and QMC	Update

Allows everyone that can see an app to see it's content files

Name	Resource filter	Conditions	Context	Actions
ReadAppContentFiles	StaticContentReference_*	resource.AppContents.App.HasPrivilege("Read")	Both in hub and QMC	Read

Allows everyone that can update an app to manage it's content files

Name	Resource filter	Conditions	Context	Actions
UpdateAppContentFiles	StaticContentReference_*	resource.AppContents.App.HasPrivilege("Update")	Both in hub and QMC	Ceate Read Update Delete

Content Library

Allows everyone that can see a content library to see its corresponding files

Name	Resource filter	Conditions	Context	Actions
Content library content	StaticContentReference_*	resource.ContentLibrarys.HasPrivilege("Read")	Both in hub and QMC	Read

Allows everyone that can update a content library to manage its corresponding files

Name	Resource filter	Conditions	Context	Actions
Content library manage content	StaticContentReference_*	resource.ContentLibrarys.HasPrivilege("Update")	Both in hub and QMC	Create, Read Update Delete

Content

Allows everyone to read installed static content

Name	Resource filter	Conditions	Context	Actions
Installed static content	StaticContentReference_*	((resource.StaticContentSecurityType="Open"))	Both in hub and QMC	Read

Allows everyone that can see a shared content to see its corresponding files

Name	Resource filter	Conditions	Context	Actions
Shared content see content	StaticContentReference_*	resource.SharedContents.HasPrivilege("Read")	Both in hub and QMC	Read

Allows everyone that can update a shared content to manage its corresponding files

Name	Resource filter	Conditions	Context	Actions
Shared content manage content	StaticContentReference_*	resource.SharedContents.HasPrivilege("Update")	Both in hub and QMC	Create Read Update Delete

Allows everyone except anonymous users to create temporary content

Name	Resource filter	Conditions	Context	Actions
Temporary content	TempContent_*	!user.IsAnonymous()	Both in hub and QMC	Create

Extension

Allows everyone that can see an extension to see its corresponding files

Name	Resource filter	Conditions	Context	Actions
Extension static content	StaticContentReference_*	resource.Extensions.HasPrivilege("Read")	Both in hub and QMC	Read

Allows everyone that can update an extension to manage its corresponding files

Name	Resource filter	Conditions	Context	Actions
Extension manage content	StaticContentReference_*	resource.Extensions.HasPrivilege("Update")	Both in hub and QMC	Create, Read Update Delete

File Reference

Everyone is allowed to read file references

Name	Resource filter	Conditions	Context	Actions
ReadFileReference	FileReference_*	!user.IsAnonymous()	Both in hub and QMC	Read

Owned Resource

The owner of a resource should be able to see the resource if it is published to a stream

Name	Resource filter	Conditions	Context	Actions
OwnerRead	*	resource.IsOwned() and resource.owner = user	Both in hub and QMC	Read

User (Service Account / Root Admin)

The service accounts should be able to do all actions

Name	Resource filter	Conditions	Context	Actions
ServiceAccount	*	((user.UserDirectory="INTERNAL" and user.UserId like "sa_*"))	Both in hub and QMC	Create Read Update Delete Export Publish Change owner Change role Export data

Root admin should have full access rights

Name	Resource filter	Conditions	Context	Actions
RootAdmin	*	((user.roles="RootAdmin"))	Both in hub and QMC	Create Read Update Delete Export Publish Change owner Change role Export data

Default Security Rules

Resources

App

Everyone is allowed to create apps except anonymous users

Name	Resource filter	Conditions	Context	Actions
CreateApp	App_*	!user.IsAnonymous()	Only in hub	Create

Everyone is allowed to export the app data they are allowed to see except anonymous users

Name	Resource filter	Conditions	Context	Actions
ExportAppData	App_*	!user.IsAnonymous()	Only in hub	Export data

The user should see the resource if he/she has read access to the stream it is published to

Name	Resource filter	Conditions	Context	Actions
Stream	App*	(resource.resourcetype = "App" and resource.stream.HasPrivilege("read")) or ((resource.resourcetype = "App.Object" and resource.published ="true" and resource.objectType != "app_appscript" and resource.objectType != "loadmodel") and resource.app.stream.HasPrivilege("read"))	Both in hub and QMC	Read

App Object

If you have read rights on an published app you should be able to create sheets, stories, bookmarks and snapshots belonging to that app

Name	Resource filter	Conditions	Context	Actions
CreateAppObjectsPublishedApp	App.Object_*	!resource.App.stream.Empty() and resource.App.HasPrivilege("read") and (resource.objectType = "userstate" or resource.objectType = "sheet" or resource.objectType = "story" or resource.objectType = "bookmark" or resource.objectType = "snapshot" or resource.objectType = "embeddedsnapshot" or resource.objectType = "hiddenbookmark") and !user.IsAnonymous()	Only in hub	Create

If you have read rights on an unpublished app you should be able to create app objects belonging to that app

Name	Resource filter	Conditions	Context	Actions
CreateAppObjectsUnPublishedApp	App.Object_*	resource.App.stream.Empty() and resource.App.HasPrivilege("read") and !user.IsAnonymous()	Only in hub	Create

Content Library

The default content library should be visible for all users

Name	Resource filter	Conditions	Context	Actions
Default content library	ContentLibrary_365cddf2-1181-4204-8800-e9a46fe3b127	true	Both in hub and QMC	Read

Data Connection

It should be possible to create data connections except of type folder

Name	Resource filter	Conditions	Context	Actions
DataConnection	DataConnection_*	((resource.type!="folder"))	Only in hub	Create

It should be possible for admins to create folder data connections

Name	Resource filter	Conditions	Context	Actions
FolderDataConnection	DataConnection_*	resource.type = "folder" and (user.roles = "RootAdmin" or user.roles = "ContentAdmin" or user.roles = "SecurityAdmin")	Only in hub	Create Read Update Delete

Data connection used for uploading files to server

Name	Resource filter	Conditions	Context	Actions
File upload connection object	DataConnection_47a1cfd8-f70e-4a98-a00d-00fca6c8e253	!user.IsAnonymous()	Both in hub and QMC	Read

Extension

Everyone can view extensions

Name	Resource filter	Conditions	Context	Actions
Extension	Extension_*	true	Both in hub and QMC	Read

Stream

The default stream called Everyone should be visible for all users and all users should be able to publish to it

Name	Resource filter	Conditions	Context	Actions
StreamEveryone	Stream_aaec8d41-5201-43ab-809f-3063750dfafd	!user.IsAnonymous()	Both in hub and QMC	Read Publish

The default stream called Everyone should be visible for anonymous users

Name	Resource filter	Conditions	Context	Actions
StreamEveryoneAnonymous	Stream_aaec8d41-5201-43ab-809f-3063750dfafd	!user.IsAnonymous()	Only in hub	Read

RootAdmin, ContentAdmin and SecurityAdmin should be able to publish to the default stream called Monitoring apps

Name	Resource filter	Conditions	Context	Actions
StreamMonitoringAppsPublish	Stream_a70ca8a5-1d59-4cc9-b5fa-6e207978dcaf	((user.roles="RootAdmin" or user.roles="ContentAdmin" or user.roles="SecurityAdmin"))	Only in hub	Publish

The default stream called Monitoring apps should be visible for default Administrators

Name	Resource filter	Conditions	Context	Actions
StreamMonitoringAppsRead	Stream_a70ca8a5-1d59-4cc9-b5fa-6e207978dcaf	((user.roles="RootAdmin" or user.roles="ContentAdmin" or user.roles="SecurityAdmin" or user.roles="DeploymentAdmin" or user.roles="AuditAdmin"))	Both in hub and QMC	Read

Hub

Allows all users to access all hub sections

Name	Resource filter	Conditions	Context	Actions
HubSections	HubSection_*	true	Both in Hub and in QMC	Read

Owned Resource

The owner of a resource should be able to do Update and Delete actions if the resource is not published to a stream

Name	Resource filter	Conditions	Context	Actions
Owner	*	resource.IsOwned() and (resource.owner = user and !((resource.resourcetype = "App" and !resource.stream.Empty()) or (resource.resourcetype = "App.Object" and resource.published = "true")))	Both in hub and QMC	Update Delete

The owner of an app or a stream should be able to publish

Name	Resource filter	Conditions	Context	Actions
OwnerPublish	App_*,Stream_*	resource.IsOwned() and resource.owner = user	Both in hub and QMC	Publish

The owner of an app object should be able to publish an object unless it is approved

Name	Resource filter	Conditions	Context	Actions
OwnerPublishAppObject	App.Object_*	resource.IsOwned() and resource.owner = user and resource.approved = "false"	Both in hub and QMC	Publish

Cloud Credentials

The user should be able to create cloud credentials for the stream he/she has create access to

Name	Resource filter	Conditions	Context	Actions
CreateCloudCredentials	CloudCredentials_*	(resource.stream.HasPrivilege("create") and !user.IsAnonymous())	Both in Hub and in QMC	Create

The user should see cloud credentials if he/she has read access to the stream they are related to

Name	Resource filter	Conditions	Context	Actions
ReadCloudCredentials	CloudCredentials_*	(resource.stream.HasPrivilege("read") and !user.IsAnonymous())	Both in Hub and in QMC	Read

On-Demand App Generation (ODAG)

Non-anonymous users with read access to the ODAG template app can create links and it is possible to create a link without first knowing the template app

Name	Resource filter	Conditions	Context	Actions
CreateOdagLinks	OdagLink_*	!user.IsAnonymous() and (resource.templateApp.Empty() or resource.templateApp.HasPrivilege("read"))	Only in Hub	Create

Non-anonymous users with update access to the selectionApp and read access to the link can create OdagLinkUsages

Name	Resource filter	Conditions	Context	Actions
CreateOdagLinkUsage	OdagLink_*	!user.IsAnonymous() and (resource.selectionApp.Empty() or resource.selectionApp.HasPrivilege("update")) and (resource.link.Empty() or resource.link.HasPrivilege("read"))	Only in Hub	Create

Non-anonymous users with read access to the link can create new Requests using that link

Name	Resource filter	Conditions	Context	Actions
CreateOdagLinkUsage	OdagRequest_*	!user.IsAnonymous() and (resource.link.HasPrivilege("Read"))	Only in Hub	Create

Non-anonymous users with read access to any selection app using the ODAG link can read the link

Name	Resource filter	Conditions	Context	Actions
ReadOdagLinks	OdagLink_*	!user.IsAnonymous() and resource.OdagLinkUsage.selectionApp.HasPrivilege("read")	Only in Hub	Read

Non-anonymous users with read access to the selection app and link can read an OdagLinkUsage

Name	Resource filter	Conditions	Context	Actions
ReadOdagLinkUsage	OdagLink_*	!user.IsAnonymous() and (resource.selectionApp.HasPrivilege("read") and resource.link.HasPrivilege("read"))	Only in Hub	Read

Default Administrative User Group

Audit Admin

Audit admin should have access rights to audit related entities

Name	Resource filter	Conditions	Context	Actions
AuditAdmin	*	user.roles = "AuditAdmin" and !(resource.resourcetype = "TransientObject" and resource.name like "QmcSection_*")	Only in QMC	Read

Audit admin should have access rights to audit related sections

Name	Resource filter	Conditions	Context	Actions
AuditAdminQmcSections	License_*,TermsAcceptance_*,QmcSection_Tag,QmcSection_Audit	((user.roles="AuditAdmin"))	Only in QMC	Read

Content Admin

Content admin should have access rights to content related entities

Name	Resource filter	Conditions	Context	Actions
ContentAdmin	Stream_*,App*,ReloadTask_*,UserSyncTask_*,SchemaEvent_*,User*,CustomProperty*,Tag_*,DataConnection_*,CompositeEvent_*,Extension_*,ContentLibrary_*	((user.roles="ContentAdmin"))	Only in QMC	Create Read Update Delete Export Publish Change owner

Content admin should have access rights to content related sections

Name	Resource filter	Conditions	Context	Actions
ContentAdminQmcSections	License_*,TermsAcceptance_*,QmcSection_Stream,QmcSection_App,QmcSection_App.Object,QmcSection_DataConnection,QmcSection_Tag,QmcSection_User,QmcSection_CustomPropertyDefinition,QmcSection_Task,QmcSection_Event,QmcSection_SchemaEvent,QmcSection_CompositeEvent,QmcSection_Extension,QmcSection_ReloadTask,QmcSection_UserSyncTask,QmcSection_ContentLibrary,QmcSection_Audit	((user.roles="ContentAdmin"))	Only in QMC	Read

Content admin should have access rights to manage security rules for streams, data connections, content libraries and extensions

Name	Resource filter	Conditions	Context	Actions
ContentAdminRulesAccess	SystemRule_*	user.roles = "ContentAdmin" and resource.category = "Security" and (resource.resourcefilter matches "Stream_¥w{8}-¥w{4}-¥w{4}-¥w{4}-¥w{12}" or resource.resourcefilter matches "DataConnection_¥w{8}-¥w{4}-¥w{4}-¥w{4}-¥w{12}" or resource.resourcefilter matches "ContentLibrary_¥w{8}-¥w{4}-¥w{4}-¥w{4}-¥w{12}" or resource.resourcefilter matches "Extension_¥w{8}-¥w{4}-¥w{4}-¥w{4}-¥w{12}")	Only in QMC	Create Read Update Delete

Deployment Admin

Deployment admin should have access rights to deployment related entities

Name	Resource filter	Conditions	Context	Actions
DeploymentAdmin	ServiceCluster_*,ServerNodeConfiguration_*,Engine*,Proxy*,VirtualProxy*,Repository*,Printing*,Scheduler*,User*,CustomProperty*,Tag_*,License*,TermsAcceptance_*,ReloadTask_*,UserSyncTask_*,SchemaEvent_*,CompositeEvent_*	((user.roles="DeploymentAdmin"))	Only in QMC	Create Read Update Delete

Deployment admin should have access rights to see and update apps in order to handle sync rules

Name	Resource filter	Conditions	Context	Actions
DeploymentAdminAppAccess	App_*	((user.roles="DeploymentAdmin"))	Only in QMC	Read Update

Deployment admin should have access rights to deployment related sections

Name	Resource filter	Conditions	Context	Actions
DeploymentAdminQmcSections	License_*,TermsAcceptance_*,ServiceStatus_*,QmcSection_Tag,QmcSection_Templates,QmcSection_ServiceCluster,QmcSection_ServerNodeConfiguration,QmcSection_EngineService,QmcSection_ProxyService,QmcSection_VirtualProxyConfig,QmcSection_RepositoryService,QmcSection_SchedulerService,QmcSection_PrintingService,QmcSection_License*,QmcSection_Token,LoadbalancingSelectList,QmcSection_User,QmcSection_UserDirectory,QmcSection_CustomPropertyDefinition,QmcSection_Certificates, QmcSection_Certificates.Export,QmcSection_Task,QmcSection_App,QmcSection_SyncRule,QmcSection_LoadBalancingRule,QmcSection_Event, QmcSection_ReloadTask, QmcSection_UserSyncTask, QmcSection_Audit	((user.roles="DeploymentAdmin"))	Only in QMC	Read

Deployment admin should have access rights to manage sync and license rules

Name	Resource filter	Conditions	Context	Actions
DeploymentAdminRuleAccess	SystemRule_*	user.roles = "DeploymentAdmin" and (resource.category = "Sync" or resource.category = "License")	Only in QMC	Create Read Update Delete

Security Admin

Security admin should have access rights to security related entities

Name	Resource filter	Conditions	Context	Actions
SecurityAdmin	Stream_*,App*,Proxy*,VirtualProxy*,User*,SystemRule_*,CustomProperty*,Tag_*,DataConnection_*,ContentLibrary_*	((user.roles="SecurityAdmin"))	Only in QMC	Create Read Update Delete Publish Change owner

Security admin should have access rights to security related sections

Name	Resource filter	Conditions	Context	Actions
SecurityAdminQmcSections	License_*,TermsAcceptance_*,ServiceStatus_*,QmcSection_Stream,QmcSection_App,QmcSection_App.Object,QmcSection_SystemRule,QmcSection_DataConnection,QmcSection_Tag,QmcSection_Templates,QmcSection_Audit,QmcSection_ProxyService,QmcSection_VirtualProxyConfig,QmcSection_User,QmcSection_CustomPropertyDefinition,QmcSection_Certificates,QmcSection_Certificates.Export,QmcSection_ContentLibrary	((user.roles="SecurityAdmin"))	Only in QMC	Read

Security admin should have read rights on ServerNodeConfiguration entity

Name	Resource filter	Conditions	Context	Actions
SecurityAdminServerNodeConfiguration	ServerNodeConfiguration_*	((user.roles="SecurityAdmin"))	Only in QMC	Read