INTEGRITI HID MOBILE CREDENTIAL INTEGRATION MANUAL

INNER RANGE recommends that all Inner Range systems be installed & maintained by FACTORY CERTIFIED TECHNICIANS.

For a list of Accredited Dealers in your area refer to the Inner Range Website.
http://www.innerrange.com

Integriti HID Mobile Credential Integration

Table Of Contents

Mobile Credential Capabilities

Core Mobile Credential Capabilities

Feature	Feature Description	Ver	Y/N
Generate new credentials for a user	Create and populate newly generated credentials, in the mobile credential system, into Integriti	22	✓
Revoke credentials from Integriti	Cancel invitations for new credentials or revoke existing credentials in the mobile credential system through the user interface or by deleting the credential from Integriti or by removing the credential from the Integriti user.	22	✓
Resend Invitations from Integriti	Send users email invitations to accept new credentials in the mobile credential system.	22	✓
Automatically generate credentials for a user from Integriti	When configured Integriti automatically generates credentials for a user as soon as a change is detected for that user.	22	✓
Automatically revoke credentials for a user from Integriti	When configured Integriti automatically revokes credentials, or cancels invitations for new credentials, for a user as soon as a change is detected for that user.	22	✓
Display Connection Status to mobile credential system	Display whether Integriti is currently connected to the mobile credential system.	22	✓
Generate Alerts from Mobile Credential Events/Alarms	Automatically generate and restore Alerts tied to a specific credential or credential pool in Integriti whenever specific events/alarms are received from the mobile credential system.	22	✓
Trigger Integriti Actions on mobile credential Events/Alarms	Trigger actions to automatically occur in Integriti whenever specific events/alarms are received from the mobile credential system.	22	✓
Entity Synchronisation	A change to an Integriti user, corresponding to a user in the mobile credential system, will verify and update that user, and credentials belonging to that user, in the mobile credential system.	22	✓

Advanced Mobile Credential Capabilities

Feature	Feature Description	Ver	Y/N
Populate Configured Credential Pools	Refreshing Child Devices will automatically populate all credential pools, configured in the mobile credential system, into Integriti when run.	22	✓
Show Card Status	The current status of configured mobile credentials will be visible directly through Integriti.	22	✓
Show Credential Pool Status	The current status of the configured credential pools will be visible directly through Integriti, whether available or not available.	22	✓
64-bit Integration Server Support	The integration supports being run on the 64-bit integration server.	22	✓
Categorised Review Records	Review generated by the integration will have a different category for different event types, allowing for easy filtering of specific Integration events.	22	✓

Integriti HID Mobile Credential Integration Compatibility

Important Notes

- When migrating from the legacy cloud credential communications handler to this HID mobile credential integration, do not delete the legacy communications handler before the migration completes.
- Filters with dynamic time are not supported by the Auto Generate Credential and Auto Revoke Credential features
- To synchronise users' photos, they must be at least 130×130 pixels. Photos larger than 396×396 will automatically be resized and cropped in order to display correctly.

Licensing Requirements

Integriti HID Mobile Credential Integration requires Integriti Professional, Integriti Business or Integriti Corporate Software Edition to operate.

Additionally, the Integriti HID Mobile Credential Integration requires the 996964 Mobile Credential Management Integration license to operate.

Minimum Installed Integriti Version

The Integriti HID Mobile Credential integration is only compatible with an installation of Integriti Pro or Infiniti that is v22.1 or higher.

Tested Against

The Integriti HID Mobile Credential plugin was built and tested against the following versions of software:

- HID Origo Mobile Identities API, version 2.2

Migration from the HID Cloud Credential Communication

Sites using the existing HID Cloud Credential communication handler will have the option to migrate to the new HID Mobile Credential integration in their own time. The legacy communication handler will continue to function for existing configurations, with no changes to how it is used or configured for v22. It is, however, recommended to plan the migration to the new HID Mobile Credential integration in the near future, as the legacy communication handler will be disabled in a future update.

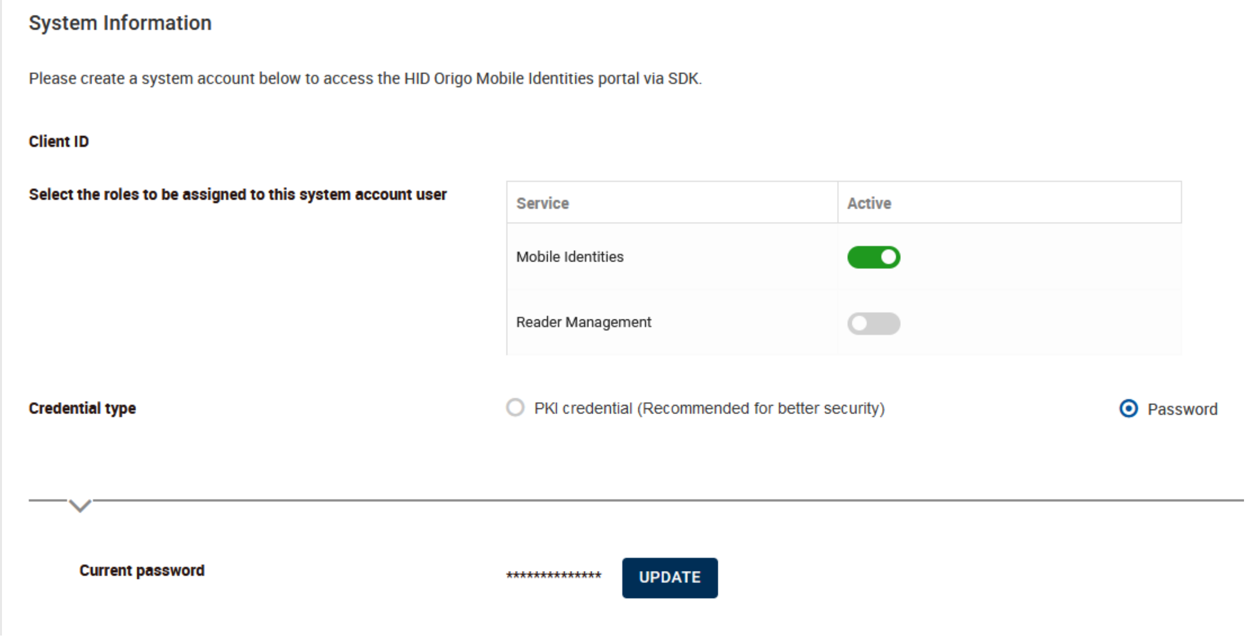
Migrating from the legacy HID Cloud Credential communication handler to the new HID Mobile Credential integration is a simple process, managed largely by the integration itself. The integration should be configured in parallel to the legacy communication handler/s, leaving the communication handler enabled. Upon refreshing child devices and starting the persisted connection of the Mobile Credential System, existing cloud credentials and user data created using the communication handler will be automatically migrated to the new format.

Once completed, the legacy communication handler will be automatically disabled, and the newly configured integration can be used going forward, with all existing mobile credentials remaining configured for management with the new integration. After the legacy communication handler has been automatically disabled, it is safe to delete it if required.

HID Configuration

HID Account Type

This section outlines the HID account type configuration required to be able to use this integration.



System Information

Please create a system account below to access the HID Origo Mobile Identities portal via SDK.

Client ID

Select the roles to be assigned to this system account user

Service	Active
Mobile Identities	☑
Reader Management	☐

Credential type ○ PKI credential (Recommended for better security) ● Password

Current password ************** UPDATE

Client ID – Gets generated for the system account by an end user.
Service – Specify service type(s) required for the account. Enable the “Mobile Identities” service to be able to generate mobile credentials through Integriti.
Credential Type – Select the “Password” credential type.

HID Credential State to Integriti Card State Mapping

This section contains a table that shows how HID Credential Status are mapped to Integriti Credential States. It also shows which card states are supported by the integration.

HID Credential Status	Integriti Card State
Issued	Active-Issued
Waiting for User to Claim (Issue Initiated)	Active-Waiting for User to Claim (Issue Initiated)
Issuing	Active - Issuing
Issuing Failure	Inactive - Issuing Failure
Revoked	Inactive - Revoked
Revoke Initiated	Inactive - Revoke Initiated
Revoking	Inactive - Revoking
Revoking Failed	Inactive - Revoking Failure
Ready for Mobile ID (Unbound)	Inactive - Ready For Mobile ID (Unbound)

Integriti Configuration

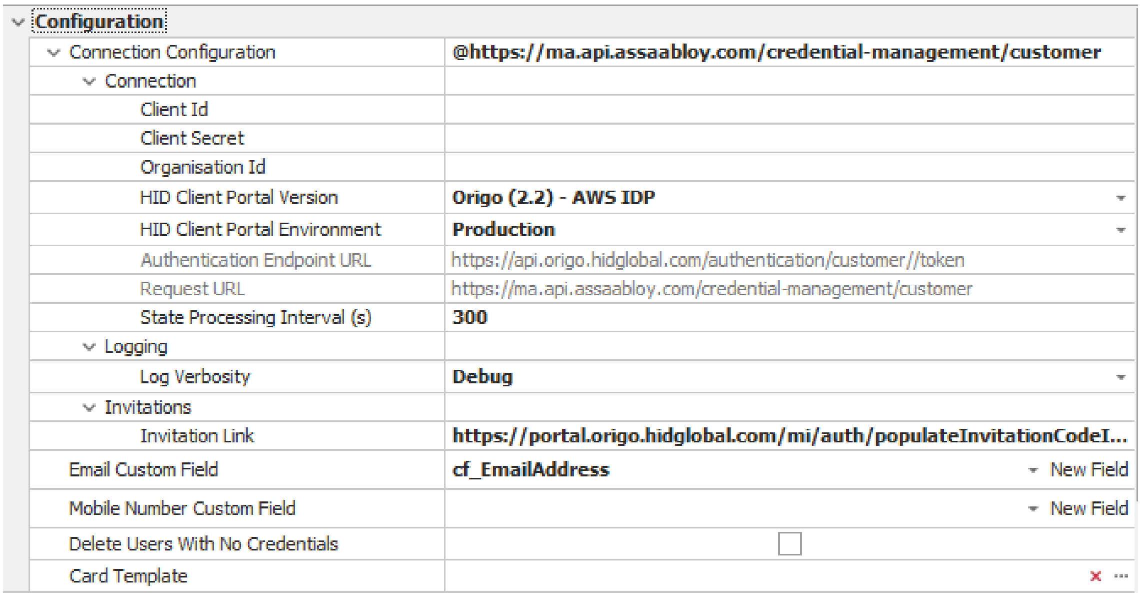
This section specifies the HID Mobile Credential Integration specific configuration details.

Ports Used

The following ports are used for communication between the Integriti HID Mobile Credential Integration and the HID Mobile Credential server. These ports should be configured in the Integriti Integration Server and any Integriti Client Machine's firewalls to allow the integration to be used.

- TCP port 443 (HTTPS)

Connection Configuration



Configuration	
Connection Configuration	@https://ma.api.assaabloy.com/credential-management/customer
Connection	
Client Id	
Client Secret	
Organisation Id	
HID Client Portal Version	Origo (2.2) - AWS IDP ▾
HID Client Portal Environment	Production ▾
Authentication Endpoint URL	https://api.origo.hidglobal.com/authentication/customer//token
Request URL	https://ma.api.assaabloy.com/credential-management/customer
State Processing Interval (s)	300
Logging	
Log Verbosity	Debug ▾
Invitations	
Invitation Link	https://portal.origo.hidglobal.com/mi/auth/populateInvitationCodeI...
Email Custom Field	cf_EmailAddress ▾ New Field
Mobile Number Custom Field	▾ New Field
Delete Users With No Credentials	□
Card Template	× ...

Connection

Client Id – Enter the User ID of the HID System account to connect to the HID Mobile Credential Service as. This is not the same as the HID management portal username. The Client Id can be found in the HID management portal under the 'System Accounts' section in the 'Administration Dashboard' page.

Client Secret - Enter the Client Secret used to authenticate the connection to the HID Mobile Credential service. This is the password configured for connecting to the HID Mobile Credential portal.

Organisation Id – Enter the Organisation/Customer Id to use for this site. This identifies which credential pools and Users will be loaded from the HID Mobile Credential service. The organisation Id is generated by HID for the organisation account.

HID Client Portal Version - Set the Client Portal Version used for this Integration. Custom - Uses the URL specified in 'Custom Request Endpoint'.

HID Client Portal Environment - Select the environment of the HID Client Portal to connect to.

State Processing Interval (s) - Select how often (in seconds) Integriti should poll for changes to card state from the HID system.

Logging

Log Verbosity - Only logs of the specified level or higher will be logged. If Warning is selected, only Warning, Error and Fatal logs will be written to the log.

Invitations

Invitation Link - Enter the Invitation Link configured in the HID Portal's Mobile Credential settings. This is only necessary if sending invitations through Integriti. The invitation code will be inserted at the end of the specified invitation link.

Email Custom Field - Select the Email Address Custom Field to use when generating credentials and sending invitations from this Mobile Credential System.
Mobile Number Custom Field - Select the Phone Number Custom Field to use when generating credentials and sending invitations from this Mobile Credential System.
Delete Users With No Credentials - Enable to automatically delete users from the 3rd party system when they no longer have any valid credentials in Integriti.
Card Template (New Credential) - Specify a Card Template to use when creating new credentials for this Integrated System or any of its children. Any new credentials created will be associated with this Card Template - Existing Credentials used by this Integrated System or its children will maintain their existing Card Template.
This can be optionally overridden for a specific child by configuring a Card Template in the child device's configuration.

Troubleshooting

Integriti is not receiving/logging card state changes	• Is persisted connection running? • Are the user Origo login credentials provided, correct? • Are the required 'Review Transitions' enabled in recorder editor? • Is the HTTPS port 443 added to the integration server's firewall? • Has persisted connection been restarted since generating the credentials?