

integriti STiD Mobile Credential Integration User Manual

[Home](#) » [integriti](#) » integriti STiD Mobile Credential Integration User Manual 

Contents

- 1 integriti STiD Mobile Credential Integration
- 2 Product Information
- 3 Product Usage Instructions
- 4 Mobile Credential Capabilities
- 5 Integriti STiD Mobile Credential Integration Compatibility
- 6 STiD Configuration
- 7 Integriti Configuration
- 8 Documents / Resources
 - 8.1 References



integriti STiD Mobile Credential Integration

Home	Manage My Account	Manage My Customer Sites	Tools and Support	Settings	Personalization Panel	Logout
Settings	Email Settings	API Settings	Credit Threshold	Private ID Settings	Transferable Settings	

API Settings

API Accessibility

☒ OAuth 2.0 (Port: 9092)

End Customer

Inner Range Sandbox

Current Status

Active

Client Id

Client Secret

Generate

Deactivate API

Product Information

The Integrati STid Mobile Credential Plugin is designed to integrate mobile credential capabilities into the Integrati system. It offers core and advanced features for managing mobile credentials efficiently.

Specifications:

- **Product Name:** Integrati STid Mobile Credential Plugin v1.1
- **Manufacturer:** Inner Range Pty Ltd
- **Location:** 1 Millennium Court, Knoxfield, Victoria 3180, Australia
- **Contact:**
 - **Telephone:** +61 3 9780 4300
 - **Email:** enquiries@innerrange.com

Product Usage Instructions

Core Mobile Credential Capabilities:

- **Generate New Credentials:** Create and populate newly generated credentials for a user in the mobile credential system, into Integrati.
- **Cancel Invitations or Revoke Existing**
- **Credentials:** Revoke credentials from Integrati either through the user interface, by deleting the credential from Integrati, or by removing the credential from the Integrati user.
- **Resend Invitations:** Send users email invitations to accept new credentials in the mobile credential system.
- **Automatically Generate and Revoke Credentials:** Automatically generate or revoke credentials for a user as soon as a change is detected for that user in Integrati.
- **Display Connection Status:** View whether Integrati is connected to the mobile credential system.

Advanced Mobile Credential Capabilities:

Entity Synchronisation:

Any change to an Integrity user corresponding to a user in the mobile credential system will update that user and their credentials in the mobile credential system.

FAQ:

- **Q: Can I use the plugin with any mobile credential system?**

A: The plugin is designed to work specifically with Integrity and may not be compatible with other mobile credential systems.

- **Q: How do I know if the plugin is successfully integrated?**

A: You can check the connection status within Integrity to see if it is connected to the mobile credential system.

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>.

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 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 STid Mobile Credential Integration Compatibility

Important Notes

- To remove virtual cards from sites in STid customers must complete the virtual card revocation process. Once a virtual card has been revoked in Integriti the end user will have to refresh their STid Mobile ID application on their mobile device to remove the virtual card from their mobile device. Only then Integriti will be able to complete the virtual card removal process.
- Virtual Card generation feature requires the persisted connection to be running.

Licensing Requirements

- The Integriti STid Mobile Credential Integration requires an Integriti/Infiniti Professional, Business or Corporate Software Edition license to be present on the product key running the integration.
- Additionally, the Integriti Mobile Credential Integration requires the 996964 Mobile Credential Management Integration license to operate.

Minimum Installed Integriti Version

The Integriti STid Mobile Credential integration is only compatible with an installation of Integriti Pro or Infiniti that is v23 or higher.

Tested Against

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

- STid Mobile ID Cloud Service v2.5.0.101

STid Configuration

Activate API, Generate Client Id and Client Secret

For Integriti to connect to STid using the STid Web Api it is necessary to activate the Api for the customer account. Once the current status of the API is 'Active' it is necessary to generate the Client ID and Client Secret. These are entered in Integriti to authenticate the connection to STid for customers to be able to use all the features offered by

the integration. This section outlines the necessary configuration steps.

The screenshot shows a web application interface with a top navigation bar containing icons and labels for Home, Manage My Account, Manage My Customer Sites, Tools and Support, Settings, Personalization Panel, and Logout. Below this is a secondary navigation bar with tabs for Settings, Email Settings, API Settings (which is underlined), Credit Threshold, Private ID Settings, and Transferable Settings. The main content area is titled 'API Settings' with a gear icon. It contains several sections: 'API Accessibility' with a radio button selected for 'OAuth 2.0 (Port: 9092)'; 'End Customer' with a dropdown menu showing 'Inner Range Sandbox'; 'Current Status' with a text field showing 'Active'; 'Client Id' with an empty text field; and 'Client Secret' with an empty text field and a copy icon. At the bottom of the form are two buttons: 'Generate' and 'Deactivate API'.

1. Open the 'API Settings' page from the 'Settings' tab.
2. Select an End Customer from the drop-down list.
3. If the 'Current Status' of the API is not active then press the 'Activate API' button.
4. Click the 'Generate' button to generate a Client Id and Client Secret.
5. The Client Secret will be shown only once so it is recommended to copy it right after generation.

Add Customer Site

To be able to add new virtual cards in STid it is necessary to create at least one customer site in STid to add the virtual cards to. This section outlines the configuration steps to create sites in STid.

Dashboard - Customer Site List

	Customer Site Name	Creation Date	Number of Configurations	Number of Users	Number of Configurators
<input type="checkbox"/>	Central Site	02-02-2022 15:22	0	1	1
<input type="checkbox"/>	Logistics Site	02-02-2022 15:23	0	0	0
<input type="checkbox"/>	Manufacturing Site	02-02-2022 15:23	0	0	1

Add

Edit

Delete

Export

1. In the 'Sites' page, under the 'Manage My Customer Sites' tab, click 'Add' to add a site to the list.

2. Specify a customer site name and click 'Create'.

Create Reader Configurations

The Integriti STid Integration requires that reader configurations are added to the relevant sites in STid to generate virtual cards in these sites. Reader configurations are created using the STid SECard software tool and imported to the STid Mobile ID portal. This section outlines the necessary steps to add a reader configuration to an STid site.

Reader Configurations

Customer Site: Manufacturing Site

PSE File Import

Search:

PSE Name	Blue Mobile ID Configuration
No matching records found	

Configuration Preview :

☐ Full Settings ☐ Reader Settings Only ☐ Chips Settings Only

Reader	OFF
MIFARE DESFire	OFF
MIFARE Plus SL3	OFF
MIFARE ClassicSL1	OFF
MIFARE UltraLight/C	OFF
Blue Mobile ID	OFF
NFC-HCE	OFF
CPS3	OFF
125 kHz	OFF
Melix code	OFF
Application Mutiservices Ctoylene (AMC)	OFF

Identification Modes

☐ Contact ☐ Very Short

☐ Up to ~ 3m ☐ Very Short

☐ Up to ~ 3m

Remote Option

☒ Remote 1 ☐ Remote 2

Save As

Assign Delete Export

1. Create a Reader Configuration using the STid SECard software tool.
2. Open the 'Reader Configurations page in the STid Mobile ID portal under the 'Manage My Customer Sites' tab.
3. From the 'Customer Site' dropdown menu select the site to add the reader configuration to.
4. Click on the 'PSE File Import' button to open the reader configuration PSE file import dialog.
5. Select the Reader Configuration PSE file for the site and click the 'Save As' button to save the configuration.
6. Repeat the above steps for all other existing STid sites.

Integriti Configuration

This section specifies the STid Mobile Credential Integration-specific configuration details. Please refer to the 'Integriti Integrations – Mobile Credential' manual for a detailed description on how to fully configure and use Mobile Credential integrations in Integriti/Infiniti.

Ports Used

The following ports are used for communication between the Integriti Stid integration and the STid 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 9092
- HTTPS Port 443

Connection Configuration

Configuration	
Integration Configuration	@secure.stidmobile-id.com
Connection	
Server Hostname	secure.stidmobile-id.com
Client Id	
Client Secret	
State Processing Interval (s)	300
Logging	
Log Verbosity	Debug
Invitations	
Invitation Link	https://secure.stidmobile-id.com/mobileid/<UID>/secure.stid...

Connection

- **Server Hostname** – The STid Mobile ID web server hostname used to connect to the STid Mobile Credential Web Service.
- **Client ID** – Enter the Client ID of the STid System account to connect to the STid Mobile Credential Service. The Client ID can be obtained from the STid account portal. Please refer to the STid Configuration section above on how to obtain the Client ID.
- **Client Secret** – Enter the Client Secret used to authenticate the connection to the STid Mobile Credential Web Service. The Client Secret can be obtained from the STid account portal. Please refer to the STid Configuration section above on how to obtain the Client Secret.
- **State Processing Interval (s)** – Select how often (in seconds) Integrati should poll for and process changes to card state from the STid 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 STid Invitation Link. This is only necessary if sending invitations through Integrati. The invitation code will be inserted in place of 'UID' in the specified invitation link.

STid Private Number Generation

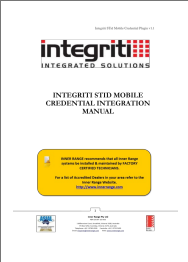
For Integrati to be able to generate a virtual card in STid it is necessary to configure the Private ID generation parameters. These parameters conform to the reader configuration specified in the STid SECard software tool. The Private ID is a unique number within the STid site. Integrati uses the options under the 'Integration Configuration' and 'Credential Generation' categories to specify the Private ID parameters. This section outlines the steps required to be able to configure the Private ID generation options.

1. Create and add STid reader configurations to STid sites as described in the 'Create Reader Configurations' section above.
2. Download the STid sites to Integrati by executing the 'Refresh Mobile Credential Pools' feature from the mobile credential system.
3. Open a credential pool in Integrati, corresponding to a STid site and reader configuration, in the 'Mobile Credential Pools' tab under 'Integrations'.
4. Specify the relevant Private ID options for the specific reader configuration that the pool corresponds to and save.

<div> <div>Configuration</div> <div> <div>Integration Configuration</div> <div>STidMobileCredentialPlugin.STidIdPoolDetails</div> <div>Send Decimal Private ID</div> <div><input checked="" type="checkbox"/></div> <div>Delete Users With No Credentials</div> <div>Inherit From Parent</div> <div>Card Template</div> <div> <div>Card Template 1</div> <div>X ...</div> </div> </div> </div>	
<div>Events/Alarms</div>	
<div>Credential Auto-Generation</div>	
<div> <div>Credential Generation</div> <div> <div>Card Start Point</div> <div>1000</div> <div>Card End Point</div> <div>10000</div> <div>Random Card Numbers</div> <div>Inherit From Parent</div> </div> </div>	
<div>Device Details</div>	
<div>Permissions</div>	

- **Send Decimal Private ID** – Specify the format Integrity will use when sending the generated Private ID to STid. If true the Private ID will be sent as a decimal number. If false Private ID will be sent as a Hexadecimal number. The format must conform to the reader configuration specified in the SECard software tool.
- **Card Start Point** – Specify the minimum number Integrity will use when generating the PrivateSTidId. This number must conform to the reader configuration specified in the SECard software tool.
- **Card End Point** – Specify the maximum number Integrity will use when generating the PrivateSTidId. This number must conform to the reader configuration specified in the SECard software tool.
- **Randomise Card Numbers** – Specify if Integrity should create a random number for Private ID. If true a random Private ID number between the ‘Card Start Point’, and ‘Card End Point’ will be generated. If false the Private ID number will be generated sequentially.

Documents / Resources

	integrity STiD Mobile Credential Integration [pdf] User Manual STiD Mobile Credential Integration, STiD, Mobile Credential Integration, Credential Integration, Integration
---	--

References

- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.