|  |
| --- |
| Indigo Instant Issuing – Group |
| Internal Technical Doc |
| Indigo release 0.1 DRAFT |

**Confidentiality**

This document is the confidential property of Veneka (Pty) Ltd and is supplied under the terms of an agreement with Veneka. It may not be disclosed or used except as is permitted by the agreement or as may be expressly permitted by Veneka (Pty) Ltd.

All registered or unregistered trademarks and service marks are properties of their respective companies and should be treated as such.

|  |  |  |  |
| --- | --- | --- | --- |
| Version. | Author | Changes | Release Date |
| 0.1 | S. Setenane | Initial Release |  |

Contents

[1 Technical configuration 5](#_Toc394151897)

[1.1 Web & Application Server 5](#_Toc394151898)

[1.2 Database 8](#_Toc394151899)

[1.3 File Loader Application 9](#_Toc394151900)

[1.4 Deployment 10](#_Toc394151901)

[12](#_Toc394151902)

[1.5 Integration 12](#_Toc394151903)

[2 Troubleshooting 13](#_Toc394151904)

[2.1 No new load batches 13](#_Toc394151905)

[2.2 Integration issues 13](#_Toc394151906)

[3 Database security 13](#_Toc394151907)

[3.1 Background 13](#_Toc394151908)

[3.2 Backup 13](#_Toc394151909)

[3.3 Restore 14](#_Toc394151910)

# Technical configuration

## Web & Application Server

### Responsibilities of Web and Application Servers

#### Web Server

The Web Server is responsible for managing the user experience, screen flow and presentation.

#### Application Server

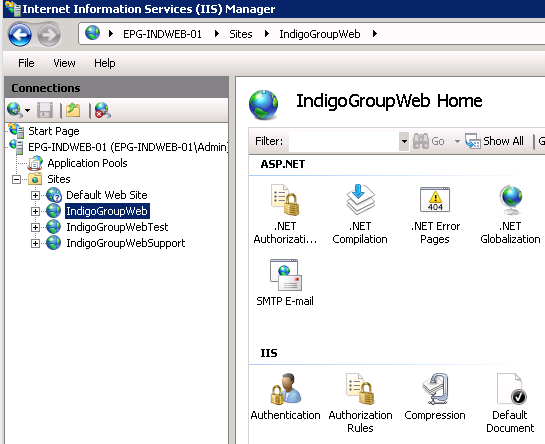
The Application Server is responsible for authenticating users and establishing and managing user sessions between the Web Server and the Application Server

The Application Server manages all connectivity to the SQL data base, thus all data reads and writes are processed via the Application Server

The Application Server interfaces with Flexcube to validate an account number.

The Application Server interfaces with CMS Card suite to link card to an account in CMS.

### Installation & Configuration

The Web and Application Servers are installed and configured in IIS. The IIS’s standard / default settings have not been changed.

As this is not an externally facing web application no additional web security has been set up.

#### Web pages

The Web Server runs as:

* 10.2.115.15:8444/default.aspx – Test Environment
* 10.2.115.15:8443/default.aspx – UAT Environment
* 10.2.115.15:8446/default.aspx – Production Support Environment

These are the URLs that we’ll be using for our three different environments to login to the system.

The Application Server runs as:

* 10.2.115.16:8444/IndigoWebService.asmx – Test Environment
* 10.2.115.16:8443/IndigoWebService.asmx – UAT Environment
* 10.2.115.16:8446/IndigoWebService.asmx – Production Support Environment

Each of these environment Have config files that specifies where the database, and logging files are.

Logging config values:

* value="C:\veneka\indigo\_group\logs\ – UAT Environment
* value="C:\veneka\indigo\_group\_test\logs\ – Test Environment
* value="C:\veneka\indigo\_group\_support\logs\ – Production Support Environment

Database config values:

* <add key="BaseConfigDir" value="C:\veneka\indigo\_group \" /> – UAT Database
* <add key="BaseConfigDir" value="C:\veneka\indigo\_group\_test\" /> – Test Database
* <add key="BaseConfigDir" value="C:\veneka\indigo\_group\_support\" /> – Support Database

These are the URLs that the Web Server uses to connect to the Application server. This URLs are not used by the users, and merely exposes the Application services that the Web Server uses.

#### Ecobank Group Deployments

When releases are made, they are password zipped and deployed into a google Drive folder name ‘Ecobank Group Deployments’.

* Google Drive Address: <https://drive.google.com/folderview?id=0B26sgINd3DXLZnZDekh4SlpvQkk&usp=sharing>
* Unzipping Password: Jungle01$

The ideal process for deploying these release are:

1. Deployed and test in the test environment so that testing and bug fixing does not affect UAT.
2. Once the new release is stable in test, it is then graduated to UAT where the Ecobank UAT Team will test and sign-off the functionality for Production.
3. Once the release has been deployed to Production, it is graduated to the Production Support Environment.

#### Servers and Logons

* Application Server – Test
  + IP Address: 10.2.115.16
  + Username: EPG-INDAPP-01\Admin
  + Password: 3c0bank3P1
* Web Server – Test
  + IP Address: 10.2.115.15
  + Username: EPG-INDWEB-01\Admin
  + Password: 3c0bank3P1
* Database Server – Test
  + IP Address: 10.2.115.17
  + Username: ECOBANKGROUP\indigoicpp
  + Password: 56Gy6]7x5m6

#### Installation directories

The Web Server has been installed in:

* C:\inetpub\IndigoGroupWebTest – Test Environment
* C:\inetpub\IndigoGroupWeb – UAT Environment
* C:\inetpub\IndigoGroupWebSupport – Production Support Environment

The Application Server has been installed in:

* C:\inetpub\IndigoGroupAppTest – Test Environment
* C:\inetpub\IndigoGroupApp – UAT Environment
* C:\inetpub\IndigoGroupAppSupport – Production Support Environment

### Error Logs

Error and system logs for the Web Server can be found in:

* C:\Veneka\indigo\_group\logs\web – UAT Environment
* C:\Veneka\indigo\_group\_test\logs\web – Test Environment
* C:\Veneka\indigo\_group\_Support\logs\web – Production Support Environment

Error and system logs for the Application Server can be found in:

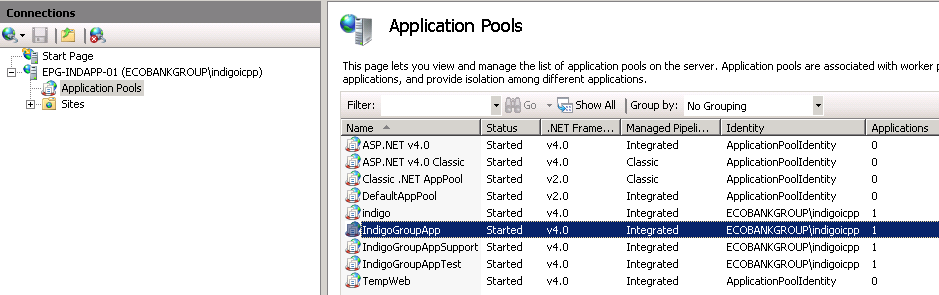
* C:\Veneka\indigo\_group\logs\app – UAT Environment
* C:\Veneka\indigo\_group\_test\logs\app – Test Environment
* C:\Veneka\indigo\_group\_Support\logs\app – Production Support Environment

Errors are written to a dated log file, and within the log file the errors are time stamped.

### Application pool setup

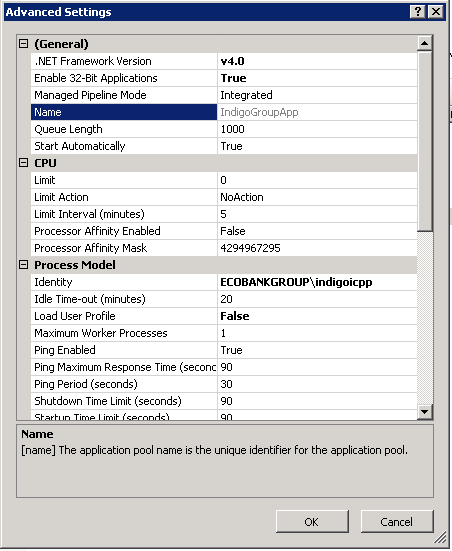
Both the Web Server and the Application server run in the indigo application pool and must be set to 4.0.

This application pool runs with the **credentials to allow access to the SQL database**.



The identity of the application pool is a user which is the correct permissions within SQL.

It is key that “Enable 32-bit Applications” is set to True for this application to run correctly.



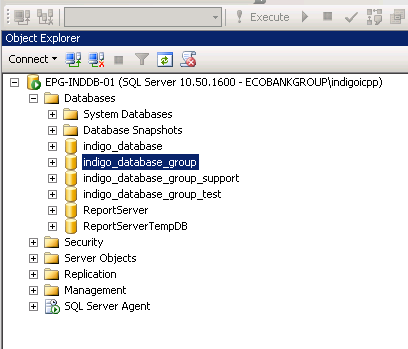
## Database

There are three databases for each environment.

### Database name

The indigo group database names are

* indigo\_database\_group – UAT Environment
* indigo\_database\_group\_support – Production Support Environment
* indigo\_database\_group\_test – Test Environment



### Database access & users

Indigo uses Windows authentication to connect to SQL.

It is only the Application Server that connects to SQL, not the individual users, therefore SQL needs to have the Windows user that the Application Server is going to log on as correctly permission-ed.

Individual users do not need to be given permission to the database.

### Database backup

Before making any database changes, the database must be backed up and placed in the database back up folder.

* Database Backup folder: C:\Veneka\db\backup

## File Loader Application

The file loader application is responsible for importing Cards files into the Indigo database. The application runs as a Windows Console App.

The app has been installed in:

* C:\Veneka\indigo\_group\CardFileLoadRunner – UAT Environment
* C:\Veneka\indigo\_group\_test\CardFileLoadRunner – Test Environment
* C:\Veneka\indigo\_group\_support\CardFileLoadRunner – Production Support Environment

The application will read in all files in Indigo group’s import directory, process the files and then move them to an archive folder.

The import directory is set up in Issuer Management, and has been configured as:

* C:\Veneka\indigo\_group\card\_files – UAT Environment
* C:\Veneka\indigo\_group\_test\card\_files – Test Environment
* C:\Veneka\indigo\_group\_support\card\_files – Support Environment

Three archive folders are used:

* \decrypted\_files
* \failed

The business rules:

1. If a file and all its records is successfully loaded, it is moved to *decrypted\_files*
2. If some of a files records are loaded, and others fail (duplication of a matching card number which already exists in the DB), then the file is moved to *failed*
3. If none of the records are loaded, the file is moved to *failed*
4. If the file name already exists in the DB, the file is moved to *failed*
5. If the file name, or its records are incorrectly formatted, then it is moved to *failed*
6. If a file is not a valid text file then it is moved to *failed*

### Error Logs

The error log is located in

* C:\Veneka\indigo\_group\logs\FileLoader – UAT Environment
* C:\Veneka\indigo\_group\_test\logs\FileLoader – Test Environment
* C:\Veneka\indigo\_group\_support\logs\FileLoader – Production Support Environment

### Application Keys

The application uses PGP decryption to decrypt batch files, which involves two key files (PrivateKey and PublicKey) and a pass phrase.

These are located under the following folders on the App Server Test and Production, respectably: 10.115.16 and 10.2.108.159

* PGP Keys
  + C:\Veneka\indigo\_group\config\ – UAT Environment
  + C:\Veneka\indigo\_group\_test\config\ – Test Environment
  + C:\Veneka\indigo\_group\_support\config\ – Production Support Environment

## Deployment

### Browser

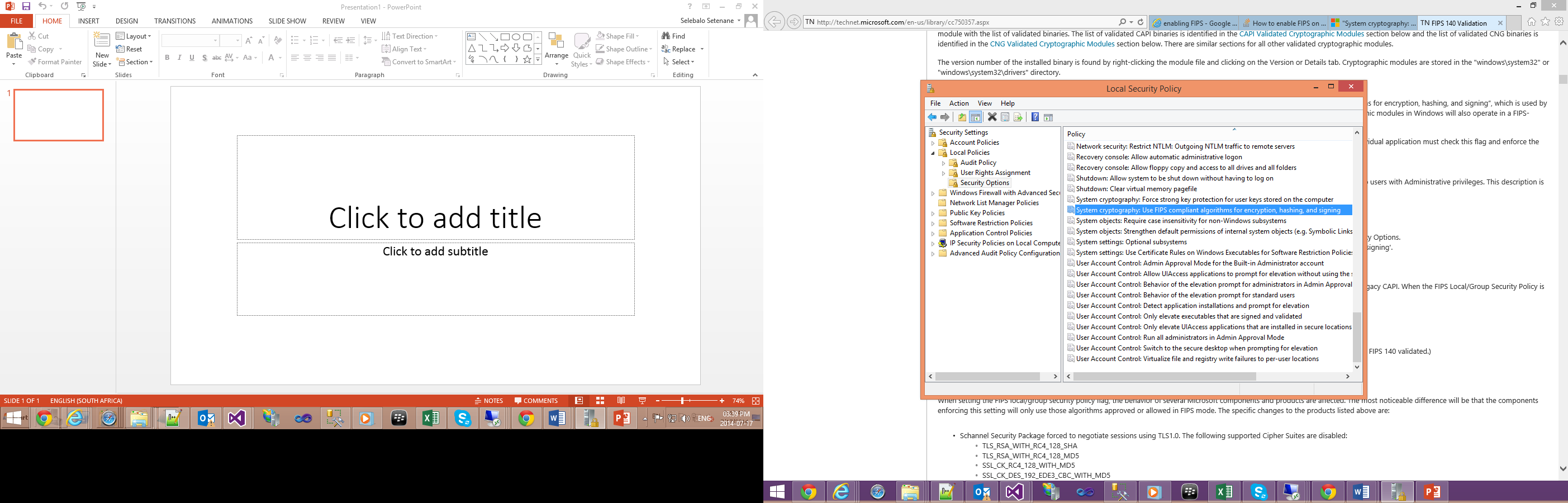
The application is being served over Citrix for security purposes.

* Citrix Url: <https://accessapp.ecobank.group/Citrix/XenApp/auth/login.aspx>
* Browser: Firefox version 3.6.19

### Enabling FIPS

FIPS must be enabled on both the Web and the App servers. Follow these steps to enable FIPS

* Open the 'Run' menu by pressing the combination 'Windows Key + R'.
* Type 'secpol.msc' and press 'Enter' or click the 'Ok' button.

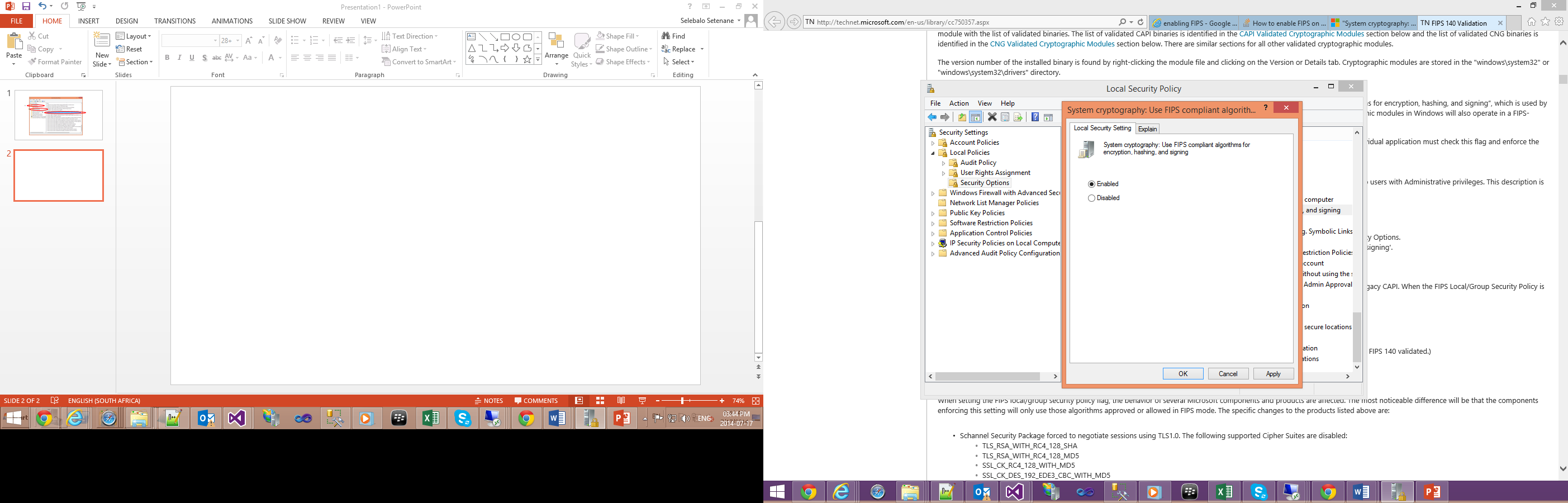


**21**

**2**

**3**

## 



**1**

## Integration

The integration for Indigo Group is handled at Database level.

* CMS Integration:

|  |  |  |
| --- | --- | --- |
| **Table Name** | **Field** | **Test Values** |
| connection\_parameters | IP Address | 10.2.115.43 |
| connection\_parameters | Port | 8443 |
| connection\_parameters | Path | /issuingws\_eco\_test/services/Issuing |
| connection\_parameters | Username | venekatest |
| connection\_parameters | Password | test123 |
| mod\_interface\_account\_params | BANK\_C | <ISSUER SPECIFIC> |
| mod\_interface\_account\_params | GROUPC | <ISSUER SPECIFIC> |
| mod\_interface\_account\_params | CYCLE | <ISSUER SPECIFIC> |
| mod\_interface\_account\_params | REP\_LANG | <ISSUER SPECIFIC> |
| product\_currency | product\_id | <PRODUCT SPECIFIC> |
| product\_currency | currency\_id | <PRODUCT SPECIFIC> |
| mod\_interface\_cond\_accnt | product\_id | <PRODUCT SPECIFIC> |
| mod\_interface\_cond\_accnt | CCY | <PRODUCT SPECIFIC> |
| mod\_interface\_cond\_accnt | COND\_SET | <PRODUCT SPECIFIC> |

* Flexcube parameters and configuration

|  |  |  |
| --- | --- | --- |
| **Table Name** | **Field** | **Test Values** |
| connection\_parameters | IP Address | 10.2.100.219 |
| connection\_parameters | Port | 5757 |
| connection\_parameters | Path | /EcoFlex |

# Troubleshooting

## No new load batches

Check the file loader activity log to see when files were last processes

Check the file loader error log to see if any errors have been recently thrown

### Follow up action:

If there are errors in the error log please raise a ticket with Veneka Support

## Integration issues

### Flexcube

All the Flexcube logs are being stored in the folder:

* C:\Veneka\indigo\_group\logs\interface\flexcube

### CMS

The full CMS error message is currently displayed to the user then there is an error linking a card to a customer.

All the CMS logs are being stored in the folder:

* C:\Veneka\indigo\_group\logs\interface\cms

These errors are usually a result of a database constraint or business logic restriction from

1. An account restriction
2. The user selecting the incorrect Issuing scenario

# Database security

## Background

The indigo database objects and data are encrypted with Triple Data Encryption Standard Algorithm (TDES) which is a symmetric-block cipher.

In Microsoft SQL (MSSQL), data encryption and decryption are made possible by using a 2-factor MSSQL encryption standard using Database Master Key (DMK) which is a symmetric key (protected by a password) and an encryption database certificate.

## Backup

As part of a planned server migration or to recover from failure for business continuity the database must be periodically backed up ideally daily or according to internal data backup policies. Backing up the database involves standard database objects backup and backing up database encryption keys which will be needed before restoration takes place.

To back up the indigo DMK a system administrator or database administrator will need to run these queries against the MSSQL server hosting the indigo database with customization obviously.

USE indigo\_database\_group;

OPEN MASTER KEY DECRYPTION BY PASSWORD = ' P@ssw0rd ';

BACKUP MASTER KEY TO FILE = 'C:\Veneka\indigo\_group\indigo\_database\_DMK\_Back'

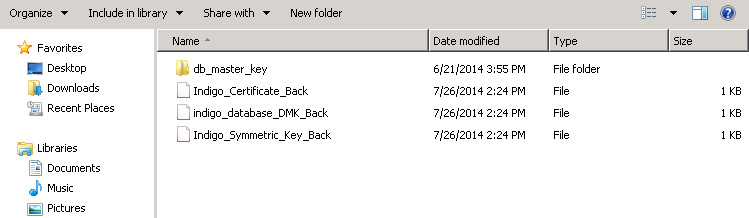
ENCRYPTION BY PASSWORD = ' P@ssw0rd ';

BACKUP CERTIFICATE Indigo\_Certificate TO FILE = 'c:\Veneka\indigo\_group\Indigo\_Certificate\_Back'

WITH PRIVATE KEY (

FILE = 'c:\Veneka\indigo\_group\Indigo\_Symmetric\_Key\_Back' ,

ENCRYPTION BY PASSWORD = 'P@ssw0rd' );

These TSQL statements will create 3 files needed for a successful restoration of the application database as shown on the screen below. 

## Restore

Please note during the master key restoration, MSSQL will decrypt all the keys encrypted by the master key to be overridden by the restored master key and this can be quite an intense operation prone to failure thus should be done when the indigo application is not used and the server’s resources are freed.

USE indigo\_database\_group;

RESTORE MASTER KEY

FROM FILE = 'c:\Veneka\indigo\_group\backups\indigo\_database\_DMK\_Back.mas'

DECRYPTION BY PASSWORD = 'Jungle01$'

ENCRYPTION BY PASSWORD = 'Jungle01$';

CREATE CERTIFICATE Indigo\_Certificate

FROM FILE = 'c:\Veneka\indigo\_group\backups\Indigo\_Certificate\_Back.cert'

WITH PRIVATE KEY (FILE = 'c:\Veneka\indigo\_group\backups\Indigo\_Symmetric\_Key\_Back.pvk',

DECRYPTION BY PASSWORD = 'Jungle01$');

After successfully executing these steps, you should be able to use the indigo database on the same machine or different machine as normal.