SMWE Managed Security Services - IAM

1.5.5

Revision History

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Effective Date (DD/MM/YYYY) | Brief Description of Change | Affected Section(s) | Prepared By | Reviewed By | Approved By |
| V 1 | 03/10/2109 | Initial draft |  | Suman Sharma, Mrinal Kant |  |  |
| V 1.2 | 20/01/2020 | Daily Health Check, Change Management, Incident Management |  | Muzibur, Mrinal, Reda |  |  |
| V 1.3 | 24/01/2020 | Team Meeting, On Call Escalation Process, Time Off Process, Team Onboarding Procedure |  | Muzibur, Mrinal, Reda |  |  |
| V 1.4 | 24/01/2020 | Logging Process with SailPoint Team with Access |  | Muzibur, Mrinal, Reda |  |  |
| V 1.5 | 24/01/2020 | Add Updates on V1.4 |  | Muzibur, Mrinal, Reda |  |  |
| V 1.5.1 | 24/01/2020 | Add Updates on V1.5 |  | Muzibur, Mrinal, Reda |  |  |
| V 1.5.2 | 27/01/2020 | Change Management updates, User Business Contact Table, URL’s, Servers, Git Setup, |  | Muzibur, Mrinal, Reda |  |  |
| V 1.5.3 | 27/01/2020 | RACI Matrix |  | Muzibur, Mrinal, Reda |  |  |
| V 1.5.4 | 15/04/2020 | Release Management, Tomcat SSL setup, Patch/eFix/Upgrade, Add updates on V 1.5.3 |  | Velavar, Gourav, Pragati, Muzibur |  |  |
| V 1.5.5 | 15/05/2020 | Address Review comments |  | Velavar |  |  |

Table of Contents

[1 Overview 5](#_Toc41444819)

[2 Scope 6](#_Toc41444820)

[3 Identity and Access Management Service 7](#_Toc41444821)

[3.1 Standard operation of IAM 7](#_Toc41444822)

[3.2 Application Product 7](#_Toc41444823)

[3.3 Users / Business Contacts 7](#_Toc41444824)

[3.4 URLs 7](#_Toc41444825)

[3.4.1 Load Balance 7](#_Toc41444826)

[3.4.2 Servers 7](#_Toc41444827)

[3.5 Daily Health Monitoring 8](#_Toc41444828)

[3.6 Performance Monitoring 8](#_Toc41444829)

[3.7 Capacity monitoring 8](#_Toc41444830)

[3.8 Change Management 8](#_Toc41444831)

[3.8.1 Purpose 8](#_Toc41444832)

[3.8.2 Change Request Process 8](#_Toc41444833)

[3.8.3 ServiceNow Change Management Deployment Process IT Operations 9](#_Toc41444834)

[3.8.4 Change Request Types 9](#_Toc41444835)

[3.8.5 Change Form 10](#_Toc41444836)

[3.8.6 Key Fields on the Change Request form include: 10](#_Toc41444837)

[3.8.7 Emergency Change Management Code Deployment Process 11](#_Toc41444838)

[3.9 Problem Management 11](#_Toc41444839)

[3.10 Incident Management 11](#_Toc41444840)

[3.11 Patch Management 13](#_Toc41444841)

[3.12 E-fix (Security Fix) 13](#_Toc41444842)

[3.12.1 Why e-fix Required 13](#_Toc41444843)

[3.12.2 What are the changes: 13](#_Toc41444844)

[3.12.3 Steps required to apply this E-fix: 14](#_Toc41444845)

[3.12.4 Below is the list of files with path need to place at the given path: 14](#_Toc41444846)

[3.12.5 Restart all application server instances in the IdentityIQ installation 14](#_Toc41444847)

[3.12.6 Installation Verification: 14](#_Toc41444848)

[3.13 Version Upgrade 15](#_Toc41444849)

[3.13.1 Overview 15](#_Toc41444850)

[3.13.2 Sandbox upgrade 15](#_Toc41444851)

[3.13.3 Dev (if not taken as sandbox) and Prod Upgrade: 16](#_Toc41444852)

[3.13.4 Data Clean up 17](#_Toc41444853)

[3.14 Auditing and Reporting 17](#_Toc41444854)

[3.15 Escalation Process 17](#_Toc41444855)

[3.15.1 Escalation Matrix: 18](#_Toc41444856)

[3.15.2 Hierarchical Escalation 18](#_Toc41444857)

[3.16 Adhoc Support 19](#_Toc41444858)

[3.17 Deployment Process 19](#_Toc41444859)

[3.18 Importing iiq Certs 21](#_Toc41444860)

[3.19 Backup Process 23](#_Toc41444861)

[3.20 Team Onboarding Process 23](#_Toc41444862)

[3.21 Time Off Process 23](#_Toc41444863)

[3.22 Team Meeting 24](#_Toc41444864)

[3.23 On call Escalation Process 24](#_Toc41444865)

[3.24 Login Process for SailPoint Team with Access 24](#_Toc41444866)

[3.25 Git Set-Up Steps 25](#_Toc41444867)

[3.26 Roles and Responsibilities 25](#_Toc41444868)

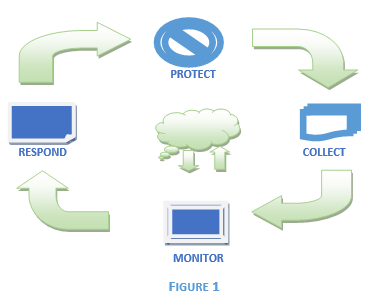
[3.27 MSS Enhancements Release Process 26](#_Toc41444869)

[3.27.1 High Level Process 26](#_Toc41444870)

[3.27.2 Process Steps 26](#_Toc41444871)

# 1 Overview

NTTDATA will provide Managed security services (MSS) as a systematic approach for managing an organization's [security](https://en.wikipedia.org/wiki/Security) needs. Functions of a managed security service include [round-the-clock](https://en.wikipedia.org/wiki/24/7_service) monitoring and management of [reported incidents](https://en.wikipedia.org/wiki/Intrusion_detection_system), overseeing [patch management](https://en.wikipedia.org/wiki/Patch-management) and [upgrades](https://en.wikipedia.org/wiki/Upgrade), performing security assessments and [security audits](https://en.wikipedia.org/wiki/Security_audit), and responding to [emergencies](https://en.wikipedia.org/wiki/Emergencies).



# 2 Scope

This document will cover the standard operating procedures for identity and access management service with the agreement between client SMWE and supplier.

# 3 Identity and Access Management Service

Customer is using SailPoint IIQ as an Identity and access management (IAM) Solution for their current environment to facilitates the user lifecycle management, group management, access controls, credential management and Policy management in their organization. Supplier will perform the below set of operation as a part of signed agreement between both the parties (NTT and Client SMWE).

## 3.1 Standard operation of IAM

## 3.2 Application Product

Software Vendor: SailPoint

Software Version: 8.0

## 3.3 Users / Business Contacts

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Martina, Rob Zavala | Marty, Gabe, Rob, Alan, Robyn | Velavar, Pragati, Gourav, Muzibur |
| Description | Business Owner | Application Administration, responsible for processing | Support/Developer |
| Email |  |  |  |
| Group | SMWE | SMWE IT, Business | NTT Data Services |

## 3.4 URLs

### 3.4.1 Load Balance

Production: <https://iamportal.stemichelle.ustis.com:8443/identityiq/>

Development: https://deviamportal:8443/identityiq/

### 3.4.2 Servers

Production Task Server: <https://172.16.201.63:8443/identityiq/login.jsf?prompt=true>

Production UI Server:<https://172.16.201.64:8443/identityiq/login.jsf?prompt=true>

Development Task Server: <https://172.16.200.94:8443/identityiq/login.jsf?prompt=true>

Development UI Server:<https://172.16.200.95:8443/identityiq/login.jsf?prompt=true>

## Daily Health Monitoring

* Check SailPoint servers are up and running
* Check latest Authoritative source file is available as per schedule
* Check All Authoritative and Non-Authoritative applications Account aggregation task status
* Check All Application Group Aggregation Task Status
* Check status of Performance Maintenance, Full refresh Task status
* Check Entitlement Extract task status
* Check the IIQ logs

## Performance Monitoring

* Performance of the application will be monitored based on the response time, transaction time, transaction break-down and error-rates.
* In case of any major degradation in performance is noticed an alert will be generated keeping all the respective participants involved.
* Windows severs team, Data base team, Application server team will be contacted.
* Proactive approach will be considered to mitigate the Performance issue immediately.

## Capacity monitoring

* It will consist of set of guidelines as recommended by SailPoint and mutually agreed between NTT and client SMWE to keep the system tuned and with the maximum peak load.
* There will be a monthly or quarterly check to keep the system tune as per business requirements.

## Change Management

### 3.8.1 Purpose

* SMWE Service Now Change Management Deployment Process

### 3.8.2 Change Request Process

All changes to servers, database management systems and enterprise applications shall be documented and approved in Service Now Change Request.

There are three type of change requests configured:

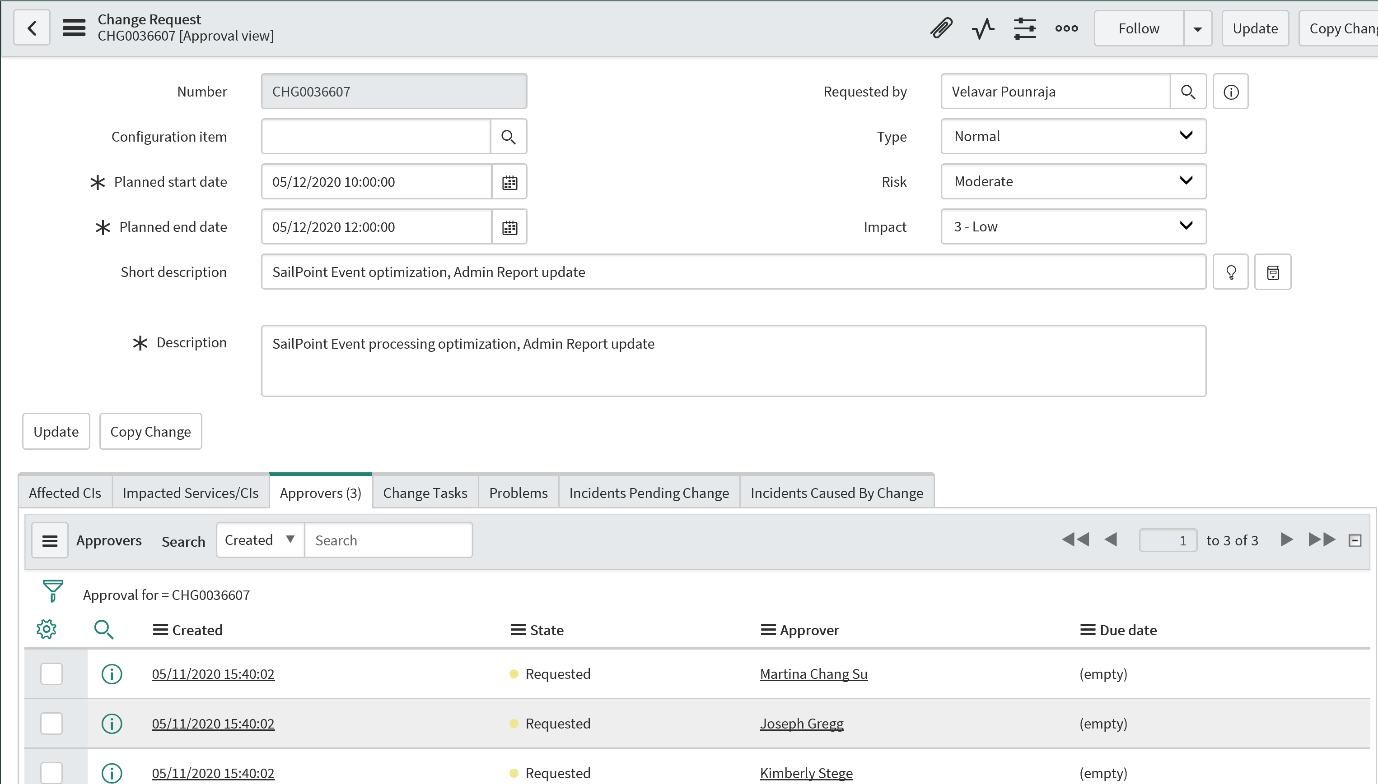
* **Standard**: Routine changes with pre-defined change plans. These are often pre-approved.

Daily audit reports

* **Normal**: Changes without predefined change plans
* **Emergency**: Unplanned changes necessary to restore service

### 3.8.3 ServiceNow Change Management Deployment Process IT Operations

CM is raised in the Service Now tool as below and Requested for Approval; The changes implemented in a week are listed in the Weekly Status report. Approvers are as listed in below for SMWE (Approval from one of the 3 approvers is sufficent to proceed with the implementation).



### 3.8.4 Change Request Types

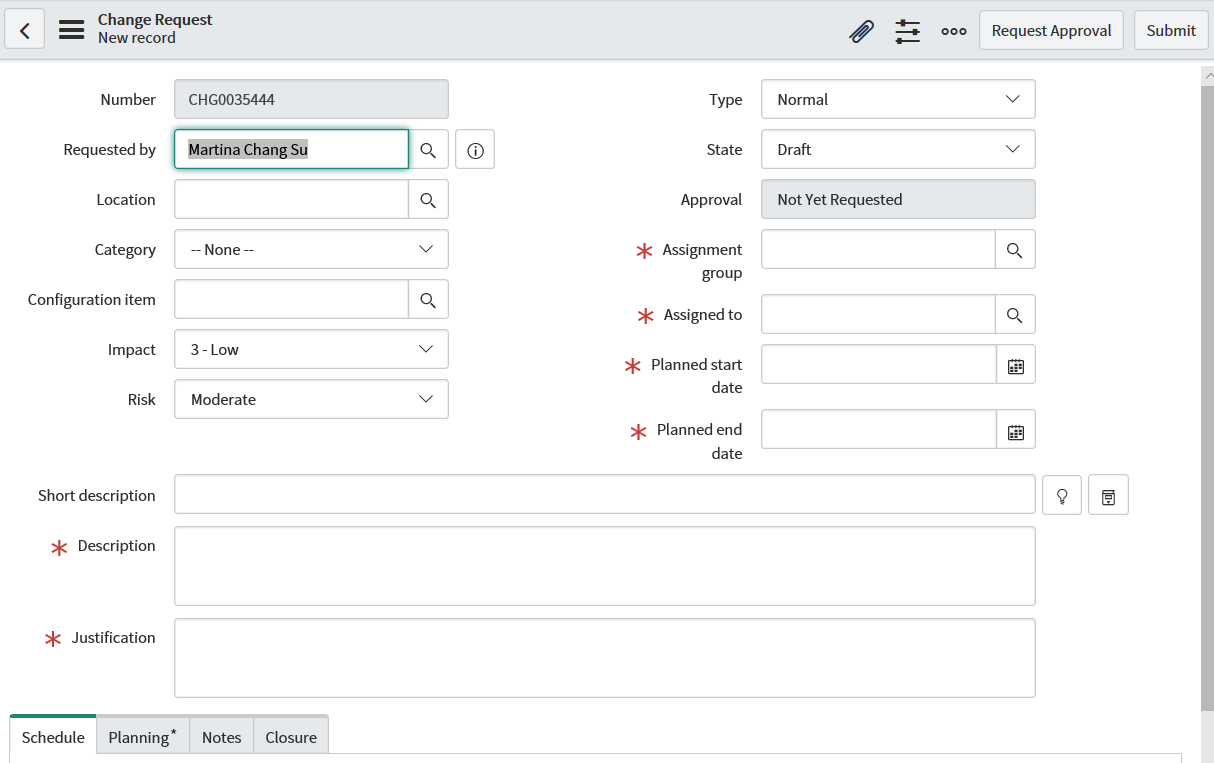
In Service Now, on the Navigation panel select Change, create new

A Change Request form will appear. There are three types of changes:

* **Standard**: Routine changes with pre-defined change plans. These are often pre-approved.Daily audit reports
* **Normal**: Changes without predefined change plans
* **Emergency**: Unplanned changes necessary to restore service

### 3.8.5 Change Form

The Change Request Form looks very similar to the Problem and Incident Forms. As with the other forms, some fields will pre-populate based on the initial information you provided.



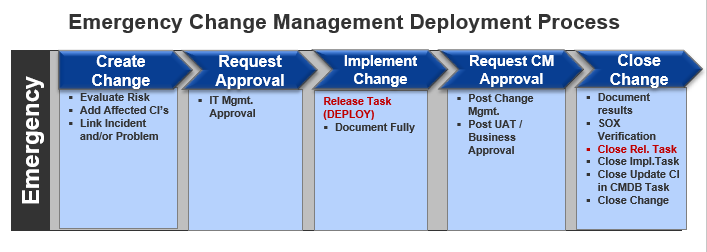
### 3.8.6 Key Fields on the Change Request form include:

**Change Tab:**

* Number – Starts with CHG and is the unique identifier of the Change
* Type – By default is set to Normal, it can be manually changed to Emergency as needed.
* Requested By
* Approval – Defaults to Not yet Requested
* Location –
* Category / Sub-Category – Further identifies the change
* Configuration Item – CI selected must be flagged as Deployable Application
* Assignment Group – Group implementing the change
* Assigned To – Person implementing the change
* Planned Start Date – Change window
* Planned End Date – Change window
* Description – Describe the change being implemented
* Justification – Purpose of the change

### 3.8.7 Emergency Change Management Code Deployment Process

The Emergency Change Management Process is used when there is an urgent business need that needs to be addressed. They are usually triggered in response to an incident or problem. An Emergency Change Request must be created and approved by the IS Manager prior to Production implementation. Change Management Team and Business Approvals are provided after Production implementation.



## Problem Management

* Problem management will include activities required to diagnose the root cause of incidents and determine the permanent resolution steps that should be taken.
* It is also responsible for ensuring that any resolutions are implemented as per the SailPoint guidelines, safely and effectively in accordance with change management and release management policies and procedures.
* These activities will be documented in Service Now ticket, while addressing tickets; if new enhancement is required, it is maintained in a Master Enhancement list document.

## Incident Management

NTTDATA will provide the IAM Baseline Support Services with the support coverage described below



* On-Call Support during the hours described below (Priority 1 Incidents and Priority 2 Incidents)
* Dedicated 9x5 support covering Client’s standard business hours (8:00 AM to 5:00 PM PT Monday through Friday) (“Business Hours”)
* On-call support for Priority 1 Incidents and Priority 2 Incidents delivered from India covering 5:00 PM through 8:00 AM PT on weekdays and 24 hours on weekends
* Seamless communication between Client, and onshore and offshore Supplier teams

Supplier will address each Incident ticket per the following priority categorization and in accordance with the Service Levels described below. Client will categorize each Incident ticket reported by Client.

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident Categorization** | **Description** | **Response Time** | **Resolution Time** |
| Priority 1(Critical) | A Critical Impact Incident exists when the SailPoint IIQ Solution or part of the SailPoint IIQ Solution is unavailable or severely degraded for multiple Authorized Users; or an incident occurs that has major actual business impact. Critical Impact Incidents must be worked on a 24-hour x 7-day basis until resolved. | 15 Minutes | 4 Hours |
| Priority 2(Major) | A Major Impact Incident is any incident that may not be classified as a Critical Impact Incident and exists when (i) the SailPoint IIQ Solution or part of the SailPoint IIQ Solution is degraded for multiple Authorized Users; or (ii) the SailPoint IIQ Solution or part of the SailPoint IIQ Solution is unavailable for a single Authorized User: or (iii) has significant actual business impact. Major Impact Incidents must be worked on a 24-hour x 7-day basis until resolved. | 30 Minutes | 8 Hours |
| Priority 3(Moderate) | A Moderate Impact Incident is any incident causing a moderate interruption or degradation of the SailPoint IIQ Solution, with moderate impact to the affected Authorized Users, environment, or business operations. While immediate impact is moderate, the risk for increased impact is apparent. There may be an automated or manual contingency plan that allows those affected to achieve a level approaching normal service delivery during the event. Moderate Impact Incidents must be worked during Business Hours until resolved. | 2 Hours | 16 Business Hours |
| Priority 4 (Low) | A Minor Impact Incident is any incident causing a minor or no interruption or degradation of the SailPoint IIQ Solution, with minimum impact to the affected Authorized User, environment, or business operations. | 4 Hours | 24 Business Hours |

As used in this Project Agreement, “Response Time” begins when Supplier is notified of an Incident and ends when Supplier responds to the same. “Resolution Time” begins when Supplier is notified of an Incident and ends when Supplier determines and corrects the root cause of the Incident and the subsequently restores the functionality or technical capability of the SailPoint IIQ Solution that was affected by such Incident.

Note: Client doesn’t have a Response Time SLA currently configured in their Service Now tool and not used with any other vendor contracts. Whether changing the ticket status to ‘Active’ indicates as ‘Response’ time? is not clear.

## Patch Management

* Supplier will maintain the application with the latest Vendor Service Pack (N-1) as recommended and mutually agreed between both parties.
* Supplier will deploy patch first in DEV environment. Once successful in Dev after 1 week it should be in QA/Staging/Pre-Prod Environment.
* Once QA will test all the existing and new functionalities. Prod Patching should be planned 2-3 weeks after QA/Staging/Pre-Prod Environment.
* Supplier/ Vendor should follow SailPoint Certification Matrix for any Patch installation. This must be reviewed and approved by enterprise architect before implementing in any of the environment.
* Similar process will be applied for Version Upgrades
* E-fix is an urgent security fix from SailPoint which fixes some critical vulnerabilities and will have to be moved to Production on priority depending on the functionality impacted. The typical steps for e-fix can vary, but a sample is as given below.

## E-fix (Security Fix)

### Why e-fix Required

SailPoint has identified a vulnerability in the Lifecycle Manager Create Identity flow and Self-Service Registration feature for vertical privilege escalation and an ExtJS grid state Cross Site Request Forgery vulnerability in all releases of IdentityIQ prior to 8.1.

### What are the changes:

The fix includes product code changes packaged in e-fix format and requires deploying these changes to, and restart of, all application server instances in the IdentityIQ installation.

This security fix contains changes to the Identity Request Approve Identity Changes subprocess workflow, LCM Registration, and LCM Validate Identity Name rule.

The changes in the workflow are to use getObjectByName instead of getObject when fetching an identity and assigning it to the variable named stub, and to perform extra identity validation during the create identity process.

The change includes two rule changes. One change in the rules is to the trim the name if the identity exists. The other change to the rules is to the definition of the filter string used for counting identities.

### Steps required to apply this E-fix:

* Download the security fix file for the version of IdentityIQ in use.The security fix is compatible only with the patch level of the indicated version unless otherwise specified. [identityiq-8.0-iiqetn8680.zip](https://community.sailpoint.com/mpomh84452/attachments/mpomh84452/IIQ_SW/979.1/1/identityiq-8.0-iiqetn8680.zip)
* Extract the security fix into the root of each IdentityIQ instance in the IdentityIQ installation.

### Below is the list of files with path need to place at the given path:

Take backup if any existing file if it is same as new file.

* WEB-INF/classes/sailpoint/object/IntegrationConfig$RoleSyncHistory.class
* WEB-INF/classes/sailpoint/object/IntegrationConfig.class
* WEB-INF/classes/sailpoint/object/ProvisioningProject$1.class
* WEB-INF/classes/sailpoint/object/ProvisioningProject$FilterReason.class
* WEB-INF/classes/sailpoint/object/ProvisioningProject.class
* WEB-INF/classes/sailpoint/transformer/IdentityTransformer.class
* WEB-INF/classes/sailpoint/web/lcm/attributes/IdentityPolicyAttributesFormBuilder.class
* WEB-INF/classes/sailpoint/workflow/IdentityLibrary$LinkDifferencer.class
* WEB-INF/classes/sailpoint/workflow/IdentityLibrary$LinksInfoGenerator.class
* WEB-INF/classes/sailpoint/workflow/IdentityLibrary.class
* WEB-INF/config/identityRequestWorkflowSubs.xml
* WEB-INF/config/lcmrules.xml
* WEB-INF/config/lcmworkflows.xml
* WEB-INF/web.xml

### Restart all application server instances in the IdentityIQ installation

### Installation Verification:

For verification after installation We can go the below path and check the message. The /debug/about.jsf page in the IdentityIQ installation that is available to users assigned the System Administrator capability will provide confirmation that the security fix has been extracted and deployed into the installation. However, this feature is available only in IdentityIQ 7.3 and later.

## Version Upgrade

Each Version upgrade has to be carefully evaluated for the backward compatibility, any existing functionality that can break, effort required for the complete upgrade\validation process, downtime required etc. with the Client.

### Overview

* Current Version: 8.0
* Target Version: 8.1
* Required Upgrade Path: 8.0GA -> 8.1GA
* Managed Artifacts
  1. XML Artifacts: yes
  2. Custom Java Classes: no
  3. File System Artifacts: yes
* Post Upgrade considerations:
  1. Validation

### Sandbox upgrade

1. Shut down the server

Note: Steps 2-5 are performed to create a replica of prod in sandbox

1. Backup DB and folder
2. Save below in web folder of ssb:
   1. WEB-INF/classes/iiq.properties
   2. WEB-INF/classes/sailpoint/object/\*Extended.hbm.xml
   3. JDBC drivers in WEB-INF/lib
3. Delete all contents of the IdentityIQ installation directory tree
4. Build and deploy a clean copy of the current production IdentityIQ version in the sandbox environment like this:
5. Checkout the build environment from the version control system.
6. Perform a clean build of the current system version with the managed artifacts and deploy it to the sandbox environment.
7. Run iiq Schema command and Drop the database and recreate it using the Create scripts

NOTE: Since extended attributes have been added to the \*Extended.hbm.xml files, the correct Create scripts must be generated by running the iiq schema command; the default scripts create only the standard number of extended attributes for each object type

1. Go to iiq console >> import the init.xml file
2. Run import init-lcm.xml
3. Run import sp.init-custom.xml

Note: Steps 6-8 are performed to upgrade sandbox to required GA release

1. Back up the database and zip a copy of the IdentityIQ installation directory tree
2. Deploy the upgrade version to your sandbox file system like this (Do not use the build process for this step.):
3. For a GA upgrade, delete the entire contents of the IdentityIQ installation directory tree. Then download the war file and unjar it in the installation directory.
4. For a patch upgrade, download the jar file and unjar it in the installation directory.
5. Copy the configuration files saved in step 3 above back into the installation:
   * iiq.properties -> WEB-INF/classes
   * \*Extended.hbm.xml -> WEB-INF/classes/sailpoint/object
   * JDBC drivers -> WEB-INF/lib
6. Run the SQL upgrade scripts (DDL) and the iiq upgrade or iiq patch command

Note: next steps include SSB update process. This is required to recompile java classes, include UI related artifacts

1. When the final target version upgrade has been performed, export copies of the managed XML artifacts from the upgraded system and copy them into the config folder of the build environment structure. This ensures that all object modifications made by the upgrade process are reflected in the build’s set of managed XML artifacts.
2. Use the build process to build and deploy the final target upgrade version in the sandbox environment as described below:
   1. Start with the build environment structure used in previous steps.
   2. copy the patch’s jar file into the base/patch directory of the build directory structure.
   3. copy the target version’s zip file into the base/ga directory of the build directory structure.
   4. Remove any efixes from the /base/efix directory of the build directory structure.
   5. Copy updated java file (logiplex) to web directory of the build directory structure.
3. Build a war file for the target upgrade version and deploy it to the sandbox environment.
4. Restart the server and validate if upgrade is successful.

### Dev (if not taken as sandbox) and Prod Upgrade:

1. Download identityiq-8.1.zip
2. Stop the IdentityIQ application.
3. Take a backup of the DB and jar the IdentityIQ installation directory.
4. Copy WEB-INF/classes/iiq.properties to /tmp.
5. Delete all from /tomcat/webapps/identityiq directory. Unzip identityiq-8.1.zip and copy identityiq.war to /tomcat/webapps/identityiq. (jar –xvf identityiq.war)
6. Copy /tmp/iiq.properties to WEB-INF/classes.
7. Run upgrade DDL: log into mysql; source upgrade\_identityiq\_tables.mysql.
8. In WEB-INF/bin directory, run iiq upgrade
9. Build iiq8.1.war file from the SSB environment, pointing servers.properties to [Environment]. (This assumes [environment].iiq.properties exists with correct properties and that[environment].target.properties contains the appropriate token properties for token substitutions. It also assumes that the 8.1GA zip war file was dropped into the build in the sandbox upgrade preparation process.)
10. Delete all from /tomcat/webapps/identityiq directory. Copy iiq8.1.war into /tomcat/webapps/identityiq and jar-xvf iiq8.1.war.
11. Copy /tmp/iiq.properties to WEB-INF/classes.
12. Launch the console (from WEB-INF/bin: ./iiq console). Import sp.init-custom.xml. (This reloads all upgraded
13. managed XML objects.)
14. Restart the application.
15. Perform all prescribed test cases (according to documented test plan).

### Data Clean up

* Supplier will provide the support for the data clean up and initial load activities as per defined SOW.
* Technical architect will do a code review and refine it as per the requirement.
* Supplier will take care of any customization which is impacting the current infrastructure and needs a cleanup based on SailPoint recommendation with mutual agreement with the client.
* Any hard coding of credentials and server parameters should be cleaned as per Enterprise architect suggestion.
* Supplier needs to make sure the data fed in to SailPoint is as per agreed format and validity; any issues arising due to incorrect data\format\duplicates from the data feed, may require supplier to fix it at the end point systems manually and coordinate with vendor to get it updated in SailPoint.

## Auditing and Reporting

Supplier will provide required weekly and monthly reports based on the agreed SOW provided auditing and reporting features are configured based on the business use case.

## Escalation Process

* The Escalation Process will be used to ensure critical issues are raised soon enough to prevent undesirable impacts to the Project and to ensure the appropriate parties are informed and involved in critical decision-making.
* Issue will be escalated by giving background, highlighting correct data, severity of the situation (high/medium/low) and suggested solutions.
* Escalation will be documented with data points and mark all necessary actions with action-owners. Mark the action owners in the ‘To’ field while communicating the escalation by email.
* The Escalation matrix will cover all the escalation contact points, escalation paths for different escalation areas and levels.

### Escalation Matrix:

SMWE IAM Escalation path:



### Hierarchical Escalation

A Hierarchical escalation is an escalation to the appropriate IT managers for incidents that are serious in nature (such as Major Incidents), for when investigation and diagnosis or resolution and recovery steps are taking too long, proving to be difficult, or when there is concern on who the incident should be allocated to.

* Hierarchical Escalations should be performed immediately to the Service Desk or Resolver Group Manager via phone call.

## Adhoc Support

* Any critical deployment which is not covered under SOW will be counted as CR and tracked separately.
* Supplier will document and update accordingly any supporting change requests, implementation and configuration steps.
* Any enhancements in the current system which are not subject to available capacity will adhere an extended support and costs accordingly.

## Deployment Process

1. Update the target.properties file
   1. All the variables, whose value is supposed to change from environment to environment need to be stored in the target.properties file
   2. There will be multiple target.properties file, each for a specific environment. Example, dev, UAT, prod etc.
   3. Using the target.properties file, first all the XML files need to be exported
      1. This will generate the new XML files where the variable values will be converted to the variable names
      2. Then same XML files need to be committed to the SSB structure present in GitHub
      3. Once the war file is generated from that SSB structure, based on the selected environment, variable names will be replaced with the environment specific variable values

So, when we are generating war file for prod, it will contain production environment specific data

* 1. Example – Active Directory Domain Name, Application connection parameters, ServiceNow connection parameters, task server ip/name etc.

1. Generate the war file through SSB
   1. First, we need to update all the XML files with the target.properties variable names
   2. We have to include all the files related to accelerator pack
   3. After that we need to make sure that, for the required environment, all the properties files are correctly updated. Example – iiq.properties, iiqCustom.properties, target.properties etc.
   4. Update the servers.properties file and add the machine name before the required environment name.
   5. Run this command from the base folder of SSB using CMD –

|  |
| --- |
| build clean war |

* 1. Rename the war file by adding the environment and release information to it and copy it over to a dedicated location

1. Set up tomcat
   1. Install pre-requisites such as java, notepad++ etc.
      1. Care need to be taken to make sure that each of the software are of the same version across the environments
      2. Tomcat version – 9.0
      3. Java version – 1.8.0\_212
   2. Add path for each of the tomcat & java in the environment variable of the machine
   3. Install the tomcat by running the exe file
   4. Run/extract the exe file to install tomcat
   5. Update the login configuration of tomcat service with correct user credentials
   6. Create a folder for logs, file path should match with log4j2.properties file. And provide required access for the IIQ user (RW).
2. Set up SSL in tomcat
   1. A KeyStore file should be provided by the client for SSL configuration. This Key store file will contain one public and a corresponding private key file. Public key must be signed by a valid certificate authority. FQDN of the public key should be the load balanced URL to be used for IIQ.
   2. We need to place that KeyStore file in a specific location
   3. In the server.xml file of tomcat, the file path and password for the KeyStore need to be updated

|  |
| --- |
| <Connector port="8080" protocol="HTTP/1.1"             redirectPort="8443"             disableUploadTimeout="false"/>  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"            maxThreads="150" scheme="https" secure="true"            keystoreFile="%tomcat\_home%\certs\keystore.pfx"  keystorePass="tomcat"            clientAuth="false" acceptCount="100"/> |

* 1. Steps:

1. Download or get the certificate in .pfx format with the password.
2. Go to **-** C:\Program Files\Java\jdk1.8.0\_211\jre\lib\security
3. open cmd in admin mode in the above path
4. run the keytool command –

Keytool -importkeystore -srckeystore C:\Temp\Certificates\***filename***.pfx -srcstoretype pkcs12 -destkeystore cacerts (Use full file path)

1. It will prompt for destination password – changeit
2. It will prompt for source pwd – (use the pwd provided with the file)

e. Also, web.xml needs to be updated by adding below lines for HTTP to HTTPS redirection –

|  |
| --- |
| <! -- automatic redirect from HTTP to HTTPS -->  <security-constraint><web-resource-collection>  <web-resource-name>Entire Application</web-resource-name>  <url-pattern>/\*</url-pattern>  </web-resource-collection>  <user-data-constraint>  <transport-guarantee>CONFIDENTIAL</transport-guarantee>  </user-data-constraint>  </security-constraint> |

1. **Import ServiceNow certificates**
   1. Go to %JAVA\_HOME%\jdk1.8.0\_211\jre\lib\security
   2. Run below command for each of the certificates and provide a unique name for them as well–

|  |
| --- |
| keytool -importcert -keystore cacerts -storepass changeit -file C:\Development\cert\rootca.cer -alias "smwedev-servicenow-rootca" |

1. **Generate database schema update script**
   1. Copy the updated hibernate files (.hbm) for IIQ in Dev and replace the one in the production
   2. Run “iiq extendedSchema” command from $IIQ\_HOME/WEB-INF/bin location to generate the database schema update SQL script
   3. Run that extension script on IdentityIQ database to update its schema.
2. **Deploy war file in tomcat**
   1. Stop tomcat from services or shutdown.bat file
   2. Go to %TOMCAT\_HOME%\webapps
   3. Create a folder called “identityiq”
   4. Copy the war file and unzip it under identityiq folder and then delete only the war file
   5. Start the tomcat

## Importing iiq Certs

Location of the Java Trust-store: C:\Program Files\Java\jdk1.8.0\_211\jre\lib\security\cacerts

Steps to Import a Certificates:

1. Download and store the certificate files in a specific location

From IP download 3 certs,

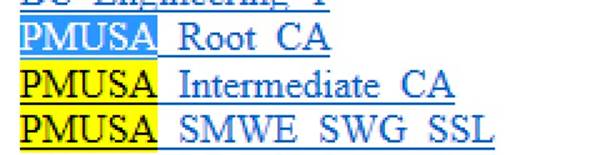
1. Open CMD in admin mode
2. Go to:\Program Files\Java\jdk1.8.0\_211\bin
3. Run keytool command –

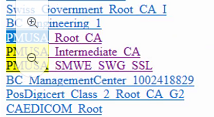
|  |
| --- |
| keytool -importcert -keystore cacerts -storepass changeit -file E:\Certs\PMUSA\_SMWE\_SWG\_SSL.cer -alias "proxy-SMWESSL" |

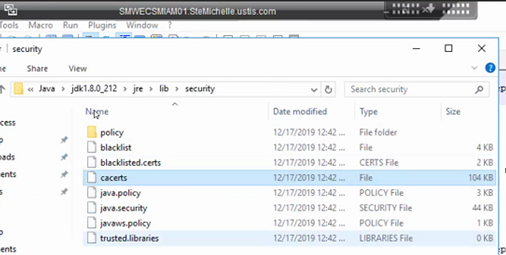
Type of Certificates to be Imported:

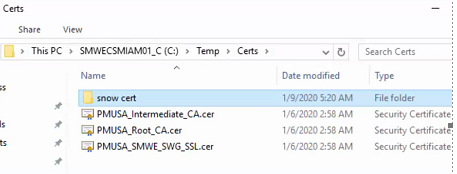
1. Proxy Certificates – Completed

<https://10.13.250.20:8082/SSL/Download_CA>



1. ServiceNow Certificates – TBD
   1. Need to be downloaded from ServiceNow production portal
   2. <https://www.ssllabs.com/ssltest/analyze.html?d=smwe.service%2dnow.com&hideResults=on&latest>
2. URL to download tomcat cert: <https://iamportal.stemichelle.ustis.com:8443/identityiq/>
3. 
4. Location of key store and certs





## [Backup Process](#_Toc21004181)

* It will be updated as per Altria DB Team Back up schedule.

## [Team Onboarding Process](#_Toc21004181)

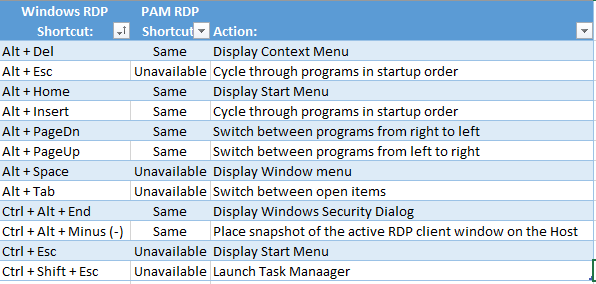
* Once NTT Data provides a background check for a new resource, the Delivery Leader raises for new joiner’s Altria ID.
* Once ID is created. New Resource raise request for IIQ, Server Access, CA PAM, Connectivity, SNOW Access.
* ALTRIA MFA Getting Started



* CA PAM Installation CSG



* CA PAM Short cuts



## [3.21 Time Off Process](#_Toc21004181)

* Any offshore resource or Onshore resource who wants to take a Plan Leave need to inform 45 days prior to Leave start date.
* Required email approval from Service Delivery Manager to apply Leave on Navigator.
* In case of sick leave or emergency leave or any unplanned leave that shift coverage will be taken care by available team member.
* Team member need to extend the shift accordingly.

## 3.22 [Team Meeting](#_Toc21004181)

* Internal Team Meeting: Scheduled Twice in a week with SDM and on need basis it might be more than twice.
* Client Team Meeting: Scheduled Weekly once as per availability of client to update weekly status report.

## 3.23 [On call Escalation Process](#_Toc21004181)

* On Call Process During Off business hours and weekends to handle the P1 and P2 Incidents 1 offshore resource will be available as per roster
* Roster is discussed with SDM and agreed with Client.
* On-call individual works issue and consults “error resolution documentation”
* Review documentation for specific application and follow notification procedure
* Contact secondary on-call or primary/secondary SME for further assistance
* Contact Manager for further escalation
* Stay in contact with Technical Support Services and user who reported the issue
* The goal for on-call is to “service restore” (get the application back up and processing) as quickly as possible. All other problems/issues will be handed off to the primary SMEs for further analysis, resolution and root cause analysis.

## 3.24 [Login Process for SailPoint Team with Access](#_Toc21004181)

**1**. To Login through VDI (for offshore)

* + Altria team will send instructions to setup the VDI
  + Call Altria Service Desk to setup the VDI
  + Altria MFA setup
  + CA PAM setup in Altria VDI
  + SMWE "c-" and "a-" account setup
  + “c-” accounts creds should be shared with employee
  + SMWE MFA setup
  + Few Software like Notepad++, winzip etc.

**2.** Login through NTT AnyConnect VPN (for offshore/Onshore)

* + URL to connect to Altria CA PAM login
  + SMWE "c-" and "a-" account setup
  + “c-” accounts creds should be shared with employee
  + SMWE MFA setup

3. Login through SMWE Laptop (onshore)

* + CA PAM client setup
  + SMWE "c-" and "a-" account setup
  + “c-” accounts creds should be shared with employee
  + SMWE MFA setup

## 3.25 Git Set-Up Steps

**Setup Steps**

1. make sure git is installed in your local; if not please raise a request and install it first. Or else you can use portable git as well, which you don’t need to install but all repositories need to be saved inside its base folder only, unless its path is added to the environment variable.
2. create a folder in your as "develop\_phase1"
3. open cmd and run --> "git clone --single-branch --branch develop\_phase1 https://github.com/pragati-rastogi/identityiq-ssb.git"
   1. May get a prompt for git credentials
   2. It will clone the develop\_phase1 branch in your local system and this will be your local git repo. Local repository will different for each individual developer.
   3. Do not clone or alter anything on the master branch. Once develop\_phase1 reaches a stable state we will merge it with the master
4. Commit the new files under --> "develop\_phase1\identityiq-ssb\ssd-v6.1\config".

**Update Steps**

1. Once the new files have been added in the folder structure, we need stage those files
   1. Command> git add .
2. After staging we need to commit the files to your local repo.
   1. Command> git commit -a -m “SCIM Integration workflows”
3. Please pull the repository again before committing. It will fetch the new changes from the remote repo/branch and merge it with your local branch.
   1. Command> git pull
4. Finally push your changes into the remote repository.
   1. Command> git push

## 3.26 Roles and Responsibilities

**The following RACI matrix identifies some key roles and responsibilities across the teams.**

R: Responsible, A: Accountable, C: Consulted, I: Informed.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IAM RACI Matrix** | | | | | | |
| **Tasks** | **SMWE Compliance Analyst** | **SMWE Tech Lead** | **SMWE ITOPS** | **JDE Team** | **ITRM Architect** | **IAM Vendor** |
| **IAM Access Re-certification / Survey Administration** | A, R | C |  | C, I |  | C, I |
| **IAM – Master Data Management / Bulk Loads** | C, I | C, I |  |  |  | A, R |
| **IAM (New functionality / systems) - User Requirements** | R | A | C, I | C, I | I | C |
| **IAM (New functionality / systems) - Architectural Design** | C, I | C, I | C, I | C, I | A, R | C, I |
| **IAM Development (New functionality / systems)** | C, I | C, I | C, I | C, I | C, I | A, R |
| **IAM Application Updates** | C, I | C, I | C, I | C, I | I | A, R |
| **IAM Processes/Reporting - Level 2 Support** | C, I | C, I | C, I | C, I | I | A, R |

## 3.27 MSS Enhancements Release Process

### 3.27.1 High Level Process

1. Global List of Enhancements
2. Prioritization
3. Estimate
4. Group into release (Quarterly release recommended).
5. Approval from SMWE
6. Source control branching for a release
7. CM
8. Testing process
9. Signoff
10. Source Control Main branch update.

### 3.27.2 Process Steps

**Global List of Enhancements**

All enhancements will be maintained in an Excel sheet and will be assigned Priority; once the Release grouping is determined, that will be updated in this sheet as well; Post release, they will be marked complete.

**Prioritization**

The enhancements list will be reviewed for status\estimate\prioritization bi-weekly with SMWE; if there is any ticket that the team hasn’t picked up for implementation, then it can be swapped out for another higher priority enhancement to include in that Release.

**Estimate**

After Prioritizing, NTT will provide estimates and propose a release grouping

Group into release (Quarterly release recommended).

SMWE will review NTT estimates and Release grouping and discuss any changes required.

**Approval from SMWE**

Once reviewed SMWE will approve the list of enhancements and the Release grouping.

**Source control branching for a release**

NTT will take a new Release branch from the Main branch and start working on the release tickets.

**Testing process**

NTT will test in DEV wherever possible and create a test plan with stakeholders to do testing in Prod after the release.

**CM**

NTT will create the CM for the Release in Prod and deployment steps documented and followed during the deployment night.

**Signoff**

SMWE completes the Test plan to verify release deployment and signs off thru email.

**Source Control Main branch update**

NTT will merge the release branch with the Main branch

**Changes to this process**

When there is another development release or an urgent P1\P2 fix etc the regular release schedule may get impacted.

When there is a security fix\patch upgrade if its not included in the release grouping, but mandated during the phase, this may also impact the release schedule.

**Tools for tracking Enhancements**

We can check if client agrees to acquire licenses for tools like TFS which is easier to track enhancements, Releases.