INFOLOCK
INSIGHT DLP APPLIANCE

IDACT QUICK START AND UPGRADE AND MIGRATION POLICY

LAST UPDATED: 2/26/2021

Prepared by:

Agyeman Danso Jr.

Manager of Technical Services

adanso@infolock.com

(202) 499-7025

TABLE OF CONTENTS

DOCUMENT CONTROL

Revision History

Version	Date	Changes	Author
1.0	11/4/2018	First Draft	Agyeman Danso
1.5	7/22/2020	Second Draft	Agyeman Danso
2.0	2/25/2021	Final Draft	Agyeman Danso

SECTION 1 INTRODUCTION

This document describes the INSIGHT DLP Appliance Configuration Tool (IDACT) policy regarding the Quick Start deployment and the Upgrade/Migration deployments for current and new customers.

This policy is subject to change based on industry requirements, so please keep an eye out for any new announcements via the support portal (support.insightdlp.com).

SECTION 1.1 TERMS AND DEFINITIONS

- **Quick Start (QST)**: Process to complete initial basic configuration of an INSIGHT Appliance(s). This will include basic configurations and does not include any advance configurations.
- **Upgrade (UPG)**: Process for patching the INSIGHT Appliance OS, and or the Symantec DLP Software, and or the Oracle DB software which resides on the INSIGHT Appliance.
- **Migrations (MIG)**: Process for moving an INSIGHT Appliance SDLP deployment to another INSIGHT Appliance(s) server. This will include basic configurations and some advance configurations.

SECTION 2 QUICK START POLICY

SECTION 2.1 INSIGHT APPLIANCE BASELINE SETUP POLICY

Infolock will perform and/or provide the following via INSIGHT Support as Baseline Setup/Basic Configurations.

INSIGHT Appliance baseline setup:

- Assistance with initial cabling of the INSIGHT Appliances.
- Assistance with initial network configuration of all identified INSIGHT Appliances.
- Assistance with initial configuration of all identified Enforce servers on all identified INSIGHT Appliances.
- Assistance with initial configuration and registrations of all identified Detection servers on all identified INSIGHT Appliances.

There will be no advance configuration included. Such as setup of Enforce backups, policies, single sign on integration, script lookups, Endpoint agents, etc. All Quick Start tasks will be in effective for a period of three (3) months after commencement of initial start date of work. If more time is required, Infolock will require customer to work with Infolock Professional Services team.

TABLE 2.2 – QUICK START BASELINE BASIC CONFIGURATION TABLE

Included	Not included
a. Setup Enforce and Detection servers	a. Setup, testing, or tuning of policies and responses rules
b. Register Detection servers and complete basic setup of the server	b. Setup or testing of any and all indexes
c. Configure system level items: Apply License, Alerts, SMTP General Setting, Users and Roles	c. Setup or testing of Discover scans
f. Endpoint: **Setup Detection server and verify it is connected to Enforce. Create and provide required Agent Package.**	d. Setup, or testing of script lookups, LDAP Lookups, Directory connections
g. Network Discover: **Setup Detection server and verify it is connected to Enforce. Verify Maximum Parallel Scans is set to no more than 8.**	e. Setup or testing of Agent Configurations

h. Network Monitor: **Setup Detection server and verify it is connected to Enforce. Verify Protocols and SPAN port are selected in server configurations.**	f. Setup or testing of Agent Groups
i. Network Prevent for Email: **Setup Detection server and verify it is connected to Enforce. Verify Maximum number of connections is set to no more than 12. Verify RequestProcessor.MTAResubmitPort and RequestProcessor.ServerSocketPort are correctly configured. Verify MTA iptables configuration is completed.**	g. Setup or testing of customized configurations. Such as backup processes, SSO, etc.
j. Network Prevent for Web: **Setup Detection server and verify it is connected to Enforce. Verify Ignore Requests/Response Smaller Than is set to no less than 512 Bytes. Verify that Maximum Number of Requests/Response and Connection Backlog are set to no more than 16.**	h. Product training, consulting involving integration, security solutions enablement, security advisory, Symantec software administration, managed security or implementation services

SECTION 3 UPGRADE POLICY

SECTION 3.1 IDACT OS UPGRADE POLICY

IDACT OS Upgrades: Infolock will perform and/or provide support for one (1) version upgrade per twelve-month period of IDACT Operating System, under the following conditions -- Customer must have a current and valid INSIGHT Support; Customer must be utilizing an INSIGHT DLP Director or Sensor Appliance; Upgrades will be performed during Standard Business Hours (Monday – Friday, 9am – 5pm ET, and excluding US federal holidays); If an afterhours upgrade is necessary, Customer is required to purchase a minimum of three (3) hours of consulting services at a rate agreed to by Infolock and Customer; and, Customer must schedule upgrade support at least ten (10) business days in advance. Note: Infolock will only perform upgrades on INSIGHT DLP Appliances. All upgrade tasks will be in effective for a period of six (6) months after commencement of initial start date of work. If more time is required, Infolock will require customer to work with Infolock Professional Services team.

SECTION 3.2 SYMANTEC DLP APPLICATION UPGRADE POLICY

Symantec DLP Application Upgrades: Infolock will perform and/or provide support for one (1) version upgrade per twelve-month period of Symantec DLP software, under the following conditions -- Customer must be entitled to the version of software to which they wish to upgrade as demonstrated by possession of a valid Symantec and/or Oracle Support Certificate; Customer must be utilizing an INSIGHT DLP Director Appliance for their Enforce/Oracle server; Upgrades will be performed during Standard Business Hours (Monday – Friday, 9am – 5pm ET, and excluding US federal holidays); If an afterhours upgrade is necessary, Customer is required to purchase a minimum of three (3) hours of consulting services at a rate agreed to by Infolock and Customer; and, Customer must schedule upgrade support at least ten (10) business days in advance. Note: Infolock will only perform upgrades for Symantec DLP software that is installed on INSIGHT DLP Appliances. All upgrade tasks will be in effective for a period of six (6) months after commencement of initial start date of work. If more time is required by Infolock will require customer to work with Infolock Professional Services team.

SECTION 3.3 ORACLE DATABASE APPLICATION UPGRADE POLICY

Oracle Database Application Upgrades: Infolock will perform and/or provide support for one (1) version upgrade per twelve-month period of Oracle Database software, under the following conditions -- Customer must be entitled to the version of software to which they wish to upgrade as demonstrated by possession of a valid Symantec and/or Oracle Support Certificate; Customer must be utilizing an INSIGHT DLP Director Appliance for their Enforce/Oracle server; Upgrades will be performed during Standard Business Hours (Monday – Friday, 9am – 5pm ET, and excluding US federal holidays); If an afterhours

upgrade is necessary, Customer is required to purchase a minimum of three (3) hours of consulting services at a rate agreed to by Infolock and Customer; and, Customer must schedule upgrade support at least ten (10) business days in advance. Note: Infolock will only perform upgrades for Oracle Database software that is installed on INSIGHT DLP Appliances. All upgrade tasks will be in effective for a period of six (6) months after commencement of initial start date of work. If more time is required by Infolock will require customer to work with Infolock Professional Services team.

SECTION 3.4 ORACLE DATABASE APPLICATION PSU PATCHING POLICY

Oracle Database Application PSU Patching: Infolock will perform and/or provide support for one (1) version PSU patching per twelve-month period of Oracle Database software, under the following conditions -- Customer must be entitled to the version of software to which they wish to patch as demonstrated by possession of a valid Symantec and/or Oracle Support Certificate; Customer must be utilizing an INSIGHT DLP Director Appliance for their Enforce/Oracle server; PSU patching will be performed during Standard Business Hours (Monday – Friday, 9am – 5pm ET, and excluding US federal holidays); If an afterhours PSU patching is necessary, Customer is required to purchase a minimum of three (3) hours of consulting services at a rate agreed to by Infolock and Customer; and, Customer must schedule PSU patching support at least ten (10) business days in advance. Note: Infolock will only perform PSU patching for Oracle Database software that is installed on INSIGHT DLP Appliances. All patching tasks will be in effective for a period of six (6) months after commencement of initial start date of work. If more time is required by Infolock will require customer to work with Infolock Professional Services team.

TABLE 3.5 – UPGRADE BASELINE BASIC CONFIGURATION TABLE

Included	Not included
a. Upgrade IDACT OS on all identified Appliance Hosts, Enforce, and Detection servers	a. Upgrade, testing, or tuning of policies and responses rules
b. Upgrade Enforce and Detection servers SDLP software	b. Upgrade or testing of any and all indexes
c. Upgrade and patch Oracle database software (if applicable)	c. Upgrade or testing of Discover scans
d. Upgrade Enforce and Detection servers	d. Upgrade or testing of script lookups, LDAP Lookups, Directory connections

e. Cloud Detect: **Verify it is connected to Enforce after upgrade. (if applicable)**	e. Upgrade or testing of Agent Configurations
f. Endpoint: **Verify it is connected to Enforce after upgrade. Create and provide required upgrade Agent Package.**	f. Upgrade or testing of Agent Groups
g. Network Discover: **Verify it is connected to Enforce after upgrade.**	g. Upgrade or testing of customized configurations. Such as backup processes, SSO, etc.
h. Network Monitor: **Verify it is connected to Enforce after upgrade.**	h. Product training, consulting involving integration, security solutions enablement, security advisory, Symantec software administration, managed security or implementation services
i. Network Prevent for Email: **Verify it is connected to Enforce after upgrade.**	
j. Network Prevent for Web: **Verify it is connected to Enforce after upgrade.**	

SECTION 4 MIGRATION POLICY

Migration of an INSIGHT Appliance server environment to another INSIGHT Appliance server environment typically occurs when moving from an EOL'd INSIGHT Appliance hardware to newer INSIGHT Appliance hardware. This will often require replication of configurations from the EOL'd INSIGHT Appliance(s) to the new INSIGHT Appliance(s). Below are the two types of migrations which can be performed. All migration tasks will be in effective for a period of six (6) months after commencement of initial start date of work. If more time is required by Infolock will require customer to work with Infolock Professional Services team.

SECTION 4.1 MIGRATION BASELINE SETUP POLICY

INSIGHT Appliance Migration baseline setup: Infolock will perform and/or provide the following via INSIGHT Support:

- Assistance with initial cabling the INSIGHT Appliances.
- Assistance with initial network configuration of all identified INSIGHT Appliances.
- Assistance with replicating configurations from previous INSIGHT Appliance deployment at best effort.

SECTION 4.2 MIGRATION ADVANCE CONFIGURATION SETUP POLICY

Symantec DLP baseline setup: Infolock will perform and/or provide the following via Symantec DLP baseline setup:

- Assistance with initial network configuration of all SDLP servers on all identified INSIGHT Appliances.
- Assistance with initial configuration of all identified Enforce servers on all identified INSIGHT Appliances.
- Assistance with initial configuration and registrations of all identified Detection servers on all identified INSIGHT Appliances.
- Assistance with replicating configurations from previous INSIGHT Appliance Symantec DLP deployment at best effort.

TABLE 4.3 – MIGRATION BASELINE BASIC CONFIGURATION TABLE

Included	Not included
a. Setup Enforce and Detection servers	a. Setup, testing, or tuning of policies and responses rules
b. Register Detection servers and complete basic setup of the server	b. Setup, migration, or testing of any and all indexes
c. Configure system level items: Apply License, Alerts, AD Authentication, Directory Connections, LDAP lookup, Saved Credentials, SMTP General Setting, Users and Roles	c. Setup, migration, or testing of Discover scans
d. Migration of active policies (if applicable from previous INSIGHT Applianec Enforce server)	d. Setup, migration, or testing of script lookups
e. Cloud Detect: **Migration of active Cloud Detection servers (if applicable from previous INSIGHT Appliance Enforce server)**	e. Setup, migration, or testing of Agent Configurations
f. Endpoint: **Setup Detection server and verify it is connected to Enforce. Create and provide required Agent Package.**	f. Setup, migration, or testing of Agent Groups
g. Network Discover: **Setup Detection server and verify it is connected to Enforce. Verify Maximum Parallel Scans is set to no more than 8.**	g. Setup, migration, or testing of customized configurations. Such as backup processes, third party SSO, etc.
h. Network Monitor: **Setup Detection server and verify it is connected to Enforce. Verify Protocols and SPAN port are selected in server configurations.**	h. Product training, consulting involving integration, security solutions enablement, security advisory, Symantec software administration, managed security or implementation services
i. Network Prevent for Email: **Setup Detection server and verify it is connected to Enforce. Verify Maximum number of connections is set to no more than 12. Verify RequestProcessor.MTAResubmitPort and RequestProcessor.ServerSocketPort are correctly configured. Verify MTA iptables configuration is completed.**	
j. Network Prevent for Web: **Setup Detection server and verify it is connected to Enforce. Verify Ignore Requests/Response Smaller Than is set to no less than 512 Bytes. Verify that**	

Maximum Number of Requests/Response and Connection Backlog are set to no more than 16.	

SECTION 5 DECOMMISION OF OLD APPLIANCE

After the competition of the Upgrade/Migration of an INSIGHT Appliance server environment to another INSIGHT Appliance server environment, typically it is recommended to decommission the old Appliance environment after all required SDLP incidents have been resolved. Until then the old INSIGHT Appliance Symantec DLP environment can remain operational as a query-only / historical reporting interface.

Described below are some useful items when decommissioning a server.

SECTION 5.1 SERVER INFO

System Name: _____

System Location: _____

Decommissioned on: _____

Make/Model	
Service Tag/ Serial #	

SECTION 5.2 GENERAL INFO

Completed	Please check appropriate boxes:
	Backups
☐	Incident Archive has been completed and removed from the Enforce server; stored in a secure location (if incident data is to be kept). Sign off: _____
	Interconnection
☐	Has the system been removed from the Active Directory tree (if applicable)?

☐	DLP Endpoint software has been removed from the related endpoint systems.
☐	DLP Prevent Web ICAP connections have been disabled from the related on-site proxies.
☐	DLP Prevent Email has been removed from the related MTAs.
	Networking
☐	IP addresses have been released back to the usable pool. Prior to release server should be shut down and disconnected from the network.
	Disk cleaning and System removal
☐	Remove the system from all monitoring processes (if applicable).
☐	Use DBAN Boot & Nuke or another secure disk wipe media, to properly wipe the system. infoLock recommends DoD wipe with a minimum of 2 passes.
☐	Update Rack/Switch labels?
	Remove Server
☐	Once the server has finished power down and unrack.

SECTION 5.3 OPERATIONAL CONTINUITY

Verify the following to account for gap coverage in DLP monitoring.

Completed	Please check appropriate boxes:
	Data-in-Motion
☐	Network Monitor egress points have been connected in the production environment.
☐	Network Prevent Web ICAP egress points configured and connected in the production environment

☐	Network Prevent Email (if configured) flow covered and replicated in the production environment.
	Data-at-Rest
☐	All data-at-rest scans have been replicated to the production system, where appropriate or have been accounted for in the production system.
	Endpoint Monitoring
☐	Endpoints configured and have been successfully uninstalled or reconnected to the production DLP installation.
	Policies
☐	Data Loss Prevention policies have been configured and enabled to monitor for data as appropriate to the production installation.