



CHARTER
VERSION 0.1

Charter - Security HLD

High-Level Design (HLD)

Document Information

Version:	0.1
Publication Date:	
Catalog Number:	document_center\2486853 Version 0.1
Information Security:	Level 1 – Confidential
Created:	7/19/2015 9:59:40 AM
Account/FOP:	Charter Communications
Author:	Mazal Shelli
Editor:	Rhoda Adler
Last Edited:	07/19/2015 10:16:34 AM
File Name:	Charter - Security HLD.docx
Template:	Development.dotm

Copyright © 2015 Amdocs.

Information Security Level 1 - Confidential

CONTAINS RESTRICTED - PROPRIETARY INFORMATION

This document is strictly confidential and proprietary; to be used only by authorized persons on a need to know basis, and must not be distributed without specific permission.

In the event of unauthorized use of this document or the confidential information it contains, violators will be subject to severe disciplinary action, based on Amdocs regulations, as well as any other sanctions applicable by law.

Table of Contents

1	Introduction	1
1.1	Purpose and Scope	1
1.2	Related Documentation	1
1.3	Terms and Definitions	2
2	Executive Summary	3
3	Amdocs Information Security	5
4	Security Solution	7
4.1	Overview	7
4.1.1	Design Guidelines	8
4.1.2	Amdocs Security Manager Overview	8
4.2	Assumptions	9
4.3	Interfaces	9
5	Users Management	10
5.1	Assumptions – N/A	10
5.2	Solution	10
5.2.1	ASM User Name Constraints	12
5.2.2	Password Management	12
6	Authentication	14
6.1	Assumptions – N/A	14
6.2	Solution	14
6.2.1	External Authentication	14
6.2.2	Consuming Amdocs Services	16
6.2.3	Consuming External Services	17
6.2.4	File Access Authentication	17
6.2.5	ASM Session Management	18
7	Authorization	19
7.1	Assumptions	19
7.2	Solution	19
7.2.1	Amdocs Security Manager	20
7.2.2	Biller Isolation APIs	21
7.2.3	Monitoring & BI	21

7.2.4	MEC	Error! Bookmark not defined.
8	Audit	24
8.1	Assumptions – N/A	24
8.2	Solution	24
8.2.1	ASM.....	24
8.2.2	Biller Isolation – APIs	25
8.2.3	Monitoring & BI.....	25
9	Confidentiality.....	26
9.1	Assumptions – N/A	26
9.2	Solution.....	26
9.2.1	Sensitive Data at Rest.....	26
9.2.2	Sensitive Data in Transit	26
9.2.3	Masking Sensitive Data on Display	26
9.2.4	Masking Sensitive Data in Logs	26
10	Infrastructure Security.....	27
10.1	Network Design	27
10.1.1	Assumptions – N/A.....	27
10.1.2	Solution	27
10.2	Users and Privilege Management	28
10.2.1	Assumptions – N/A.....	28
10.2.2	Solution	28
10.3	Logging and Auditing	28
10.3.1	Assumptions – N/A.....	28
10.3.2	Solution	28
10.4	Access Management and Data Protection	29
10.4.1	Assumptions – N/A.....	29
10.4.2	Solution	29
Appendix A	Amdocs ISO 27001 Certificate	30

1 Introduction

1.1 Purpose and Scope

The purpose of this document is to define and describe the High-Level Design (HLD) of the security solution for the Charter project.

The security solution in this document details the concepts and processes that will provide Charter with a security framework for the Amdocs system. The security approach is based on industry standards, regulations, and Amdocs leading practices coupled with Charter security requirements. Together, they form the basis for the entire security solution described in this document.

The following applications are in scope of the security solution:

- Amdocs components:
 - Ordering
 - Backend
 - REST services
 - Master Enterprise Catalog (MEC)
 - Biller Isolation
 - Search Engine
 - Operational UI
 - Web Services
- Third party component:
 - Reporting & BI (QlikView implementation)

1.2 Related Documentation

The following documents will assist the reader in obtaining a broader understanding of the subject-matter of this document:

DC#	Charter COIN Link	Document Name
2410740	TBD	Charter Billing Isolation HLS
2422470	MEC HLS	Charter – Master Enterprise Catalog (MEC) – HLS
2424187	TBD	Charter Security HLS Overview
2476119	TBD	Charter - Modify Existing Customer Flow - HLS
2424229	TBD	Charter - New Connect Order Flow - HLS

1.3 Terms and Definitions

Following is a list of terms used in this document that the reader should be familiar with:

Term	Definition
ASM	Amdocs Security Manager
BPT	Business Parameter Table
DMZ	Demilitarized Zone
EJB	Enterprise Java Beans
FE	Front end
LIC	Launched in Context
MEC	Master Enterprise Catalog
NFR	Non-functional Requirement
OOB	Out of the box
OOS	Out of scope
OS	Operating System
PEP	Policy Enforcement Point: the point in the application flow where access to a resource is checked.
RBA	Role-Based Authorization: the authorization method used in CRM
RBAC	Role-Based Access Control

2 Executive Summary

The objective of Amdocs system security includes protection of information and property from theft and corruption, while enabling the information and property to remain accessible and productive to its intended users.

The term “system security” refers to the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering, or collapse by unauthorized activities or untrustworthy individuals and unplanned events.

The security concept of the solution is based on the application’s security capabilities of Amdocs modules (which are detailed later in this chapter) in conjunction with the infrastructure’s security considerations (such as hardening) that can be performed. Moreover, consideration is given to the fact that the system (modules) operates as an independent domain within the trusted zone to which access is tightly controlled and managed via the Amdocs Security Framework at the application level, infrastructure security mechanisms, and data security on the perimeter.

The application’s security system’s building blocks (modules) are provided by the Amdocs Security Framework.

This document covers the following security measures, which are provided as part of the solution; a detailed explanation of the solution is provided in each of the relevant chapters:

Application Security

- **Users Management**

Users Management refers to the creation and management of users (human or system) in the system.

- **Authentication**

This is the process of identifying users before they are granted access to the Amdocs system (modules).

Password-based authentication is the mechanism that provide authentication in the Amdocs system solution for Charter. Any access to the Amdocs system, regardless of its calling source, is authenticated prior to having access to the system’s resources.

- **Authorization**

Authorization is the process used for determining if a requesting entity is allowed access to a resource.

The authorization in Amdocs system is based on the Role-Based Access Control (RBAC)/Role-Based Authorization (RBA) mechanism, in which each a user is assigned one or more roles. The roles define the access rights to system resources. A system resource can be, for example, a GUI element or API.

Roles are assigned to the user based on the ‘Need to Know’ concept – in accordance with the business’ needs - and must be maintained within the Amdocs system. The

authorization is governed by the internal mechanism of the modules. The mechanism is both configurable and flexible, and supports role hierarchies.

- **Accounting**

Accounting represents the process of logging an activity performed by the user.

Security events are logged in the Amdocs system by the security framework, which logs both Users Management and Authentication events, such as user creation, user update, login success/failure, and session expiration. Security logs are maintained in the system database. Every Amdocs components has its own log, where relevant operations performed in the system are logged and can be traced at a later stage.

- **Confidentiality**

Confidentiality involves the protection of information by preventing disclosure of unauthorized information.

Infrastructure Security

- **Network Design** – Placement of Amdocs system components within the network architecture.



Note: Network security elements (such as firewalls, DBF, IDS) are not in scope of this document, and are Charter's responsibility.

Typical deployment of the Amdocs system (modules) consists of several main security zones:

- DMZ/Internet access tier – containing web front end servers
- Trusted (secured) zone – includes Amdocs modules within the customer's internal network.
- DB tier – holding the solution databases
- **Users and Privilege Management** – Describes the abilities to manage users and permissions across the infrastructure components used by the Amdocs system
- **System Hardening** – Provides information of hardening capabilities of the system components:
 - Operating System (OS)
 - Database
- **Logging And Auditing** – Review of the audit capabilities and solution used by the Amdocs system at the infrastructure level
- **Access Management And Data Protection** – Describes the access management concept and the available data protection as part of the infrastructure used by the Amdocs system

3 Amdocs Information Security

Amdocs is an ISO 27001 certified organization and has established Information Security management systems and processes to ensure data security for Amdocs customers and their information assets (please see a copy of the certificate in [Appendix A](#)). The Amdocs Information Security (AIS) team is managed and led by the Amdocs Chief Information Security Officer (CISO) VP, who provides the direction and strategy to meet the path set by Amdocs Management and Board of Directors.

The AIS staff holds industry standard certifications, including but not limited to CEH, LPT, CISSP, CISM, CISA, CRISC, and AppScan Specialist.

As part of its certification, Amdocs manages security proactively and has security policies and procedures in place, including, among others:

- Information Security Policy
- Risk Assessment
- Security Incidents
- Security Awareness and Education

The Amdocs Secure Development Life Cycle (SDLC) includes security processes and procedures at every stage of the development life cycle, starting from the requirement stage up to and including design, construct, testing, (secured) deployment, and operation. The Amdocs SDLC is based on Microsoft SDL, other leading standards in the industry such as OWASP, and Amdocs' best practices.

As part of the SDLC process, Amdocs trains its employees on an application's security-related topics, which include, for example, the following development guidelines for Amdocs applications:

- The importance of security (that is, avoid security by obscurity)
- Information security training
- Correct implementation of secured coding practices to ensure the use of secure techniques
- Avoiding back doors in the system
- Prohibiting Amdocs applications client side confidential information, such as passwords.
- Error handling
- Transfer of sensitive information as a POST method
- Prohibiting the passing of sensitive information as URL parameters
- Not allowing data storage on a presentation layer
- Not trusting user inputs
- Input validation

One of the important aspects in Amdocs SDLC is the security testing that is conducted in two vectors:

- *Functional security testing* – which aims to verify that the security features of all relevant systems in scope operate correctly in accordance with the requirements.
- *Non-functional security testing* – which aims to bypass the security mechanism of the system. This consists of code scans and penetration testing performed by experts with extensive experience.



Note: Security defects are treated like any other defect in the system.

4 Security Solution

4.1 Overview

Amdocs components use Amdocs Security Manager (ASM) as their security framework. Some of the components fully adopt all its services (Authentication, Authorization, and Accounting) while others only partially adopt its services.

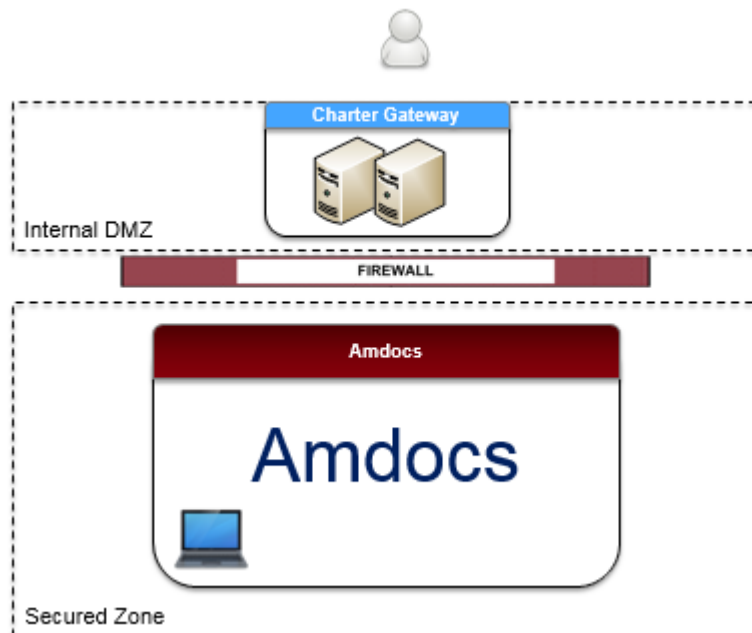
The Amdocs system operates under tightly controlled access restrictions and management through Amdocs Security Manager or the local security solution of the components. This is further detailed later in this document.

Traditionally, when looking from the security point of view, there are three different zones in the solution; however, since the Amdocs system is going to be deployed within Charter's internal network, only two zones are relevant for the solution.

- Secured zone – Includes Amdocs products (listed in section 1.1 Purpose and Scope) application servers within the Charter network.
- DMZ – Internal DMZ that hosts the Charter Gateway, which is used for any access (internal/public) to the Amdocs system.
- Web – Includes public networks (for example, the web); in this project, the Web zone is not relevant as the Amdocs system is not exposed to public networks.

The following diagram illustrates at a high level the two relevant zones, focusing on Amdocs system deployment in the production environment.

Figure 4-1: High Level Architecture



Access to the Amdocs system requires authentication. The authentication gateway to Amdocs components is via either ASM or a local mechanism (in case of third party components).

Similar to the authentication solution, authorization is also done either by ASM or by the native authorization mechanism of the component.

4.1.1 Design Guidelines

The following design guidelines were taken into consideration in providing the security solution:

- Use industry standards and regulations coupled with Amdocs leading practices, based on the out-of-the-box functionality.
- Favor cost effective solutions and assist in minimizing customization efforts.
- Minimize the security impact on system performance.

4.1.2 Amdocs Security Manager Overview

Amdocs Security Manager (ASM) provides Amdocs applications with the foundation for implementing application security topics. Its main purpose is to provide Amdocs implementations with triple “A” services in application security: Authentication, Authorization, and Accounting.

- Authentication service – The process of determining whether someone or something is in fact who or what they claim to be.
- Authorization service – The process of determining the types of activities that are permitted. Generally, authorization is in the context of authentication: once users have been authenticated, they may be authorized for different types of access or activities.
- Accounting service – The process of recording selected events or actions for later review. Audits can help in establishing patterns and noting changes in those patterns that might indicate trouble.

In addition, ASM also enables to perform user administration activities, like adding, changing the user status (active/inactive), or modifying user accounts.



Note: In this document, ‘Administration’ is referred to as ‘Users Management’.

Some system and user properties are set via the ASM configuration file (uams.properties).

Amdocs Security Manager also provides the following services:

- User account repository – A centralized physical location for storing security-related user data.
- Encryption and decryption services – APIs encrypt and decrypt sensitive information based on the preferred encryption method.
- Session control – Once a user has been authenticated, a session is created to control the authenticated user over time.

4.2 Assumptions

1. Operational security is Charter's responsibility.
2. Charter Gateway will be the security gateway to the Biller Isolation layer.
3. Charter Gateway will be the security GW to the Ordering REST services.
4. Files read by Amdocs systems are subjected to customer security restrictions – anti-virus, size check, and so on.
5. Charter is responsible for defining the authorization security model.

4.3 Interfaces

The Amdocs system interacts via the following interfaces:

- Graphical User Interfaces (GUI)
- Services
 - Inbound – Services exposed by the Amdocs system
 - Outbound – Services consumed by the Amdocs system
- File – Data files extracted/processed by the Amdocs system will reside in the secured zone.

5 Users Management

5.1 Assumptions – N/A

5.2 Solution

Users Management refers to the creation and management of users in the system.

In this solution, all users are considered internal users and can be divided into the following types:

- *Charter's employees* – administrators, analysts, designers, technicians, and so on
- *System accounts* – batch/admin users, required for supporting the functionality of the system, such as batch process users, application-to-application (Gateway) calls, and so on
- *Infrastructure users* – for example, databases, operating systems (Charter's responsibility)



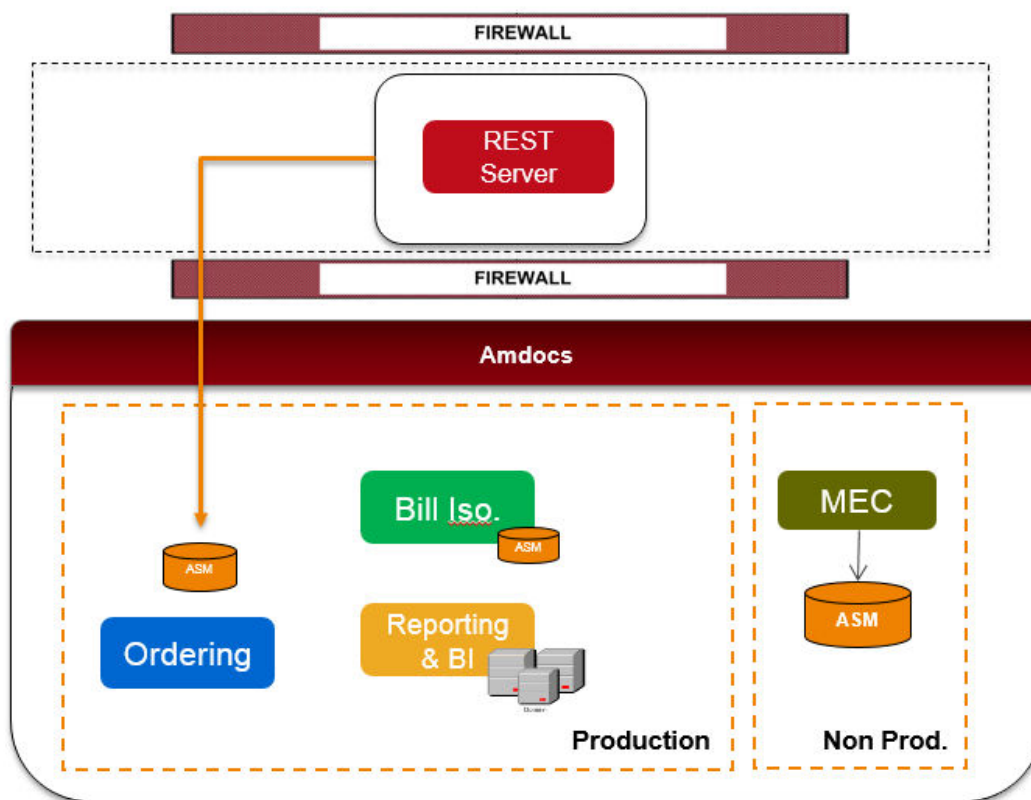
Note: Creating users in the Amdocs system and/or any users migration process is the responsibility of Charter.

This solution relies on user records stored and maintained locally within the Amdocs system repositories, either ASM or native (local) repository of the components. The solution will include the following repositories:

- ASM repositories – each of the following components will have its own instance of ASM repository:
 - Ordering
 - Biller Isolation
 - MEC
- Reporting & BI repository
- Biller Isolation Web-Services (Web Logic repository)

The following diagram depicts the user repositories in this solution.

Figure 5-1: Amdocs User Repositories in Charter Solution



The following table depicts the different user types in the system and the relevant repositories they are being maintained in.

Table 1: User Types - Repository Mapping

Users Type	ASM	Local	Charter's AD
Back office – Charter Employees	Biller Isolation (web-admin), MEC	Reporting & BI	
Back office – System Users	Ordering (BE), REST, MEC	Biller Isolation	
Back office – Infrastructure Users		Charter's infrastructure	Charter's infrastructure

All users are defined locally in the relevant repository, and each user is assigned a unique user-ID (username), password.



Note: Since Amdocs does not authenticate interactive users internally but rather does so against Charter Active Directory, Amdocs will not hold the interactive users' real passwords.

The users' records contain the security profile of the users and contain information, such as roles, time restrictions, and the number of sessions allowed for a user.

Security administration activities (for example, create user, create role) are done through the relevant security consoles:

- ASM Administration Console (MEC, Ordering)
- Web Admin Console (Biller Isolation)
- Internal Admin scripts (Biller Isolation)
- Charter Active Directory



Note: The recommendation in ASM is to not delete users from the database, but only to disable them so that their accounts are no longer active.

5.2.1 ASM User Name Constraints

The following limitations are imposed on the user name string in ASM:

- The user name must be a unique ASM object. It must not be the same as the name of another ASM object in the database.
- The user name cannot contain the colon symbol (:).
- The user name cannot contain spaces.
- The user name cannot contain invisible characters, such as tabs, Ctrl+Ms (^M), Ctrl+Vs (^V), and so on.
- Restriction on the username length is limited to 30 characters.
- The user name must not start with the following prefixes:
 - Tksmau
 - EXT

5.2.2 Password Management

In this solution, there are three different authentication provides, which in turn each is responsible for the password management of each user type.

5.2.2.1 Charter's Employees

Passwords of Charter employees that are authenticated against Charter Active Directory will not be stored in the Amdocs system. This password management is Charter's responsibility and will not be done through the Amdocs system.

5.2.2.2 System Users

System users are maintained locally within the different repositories of the system, with the exception of MEC system users.



Note: MEC system users are maintained in Charter Active Directory.

Password Management is governed internally in the relevant Amdocs system component/repository as follows:

5.2.2.2.1 Amdocs Security Manager

In ASM, passwords are stored in hash format, in accordance with common industry algorithms.

The default algorithm used by ASM is SHA2 for passwords.

ASM password policy parameters are set at the system level; that is, all users are subject to the same password policy that has been defined at the system level.

Password Management in ASM enables the Security Administrator to configure the following attributes:

- Minimum/maximum length, special characters, numeric characters, and capital and lowercase letters.
- Password history
- Password reset by a security administrator
- Password expiration time
- Lock user after X (configurable) unsuccessful login attempts
- Password reset by security administrator
- Enforce user to change his/her password after first login

5.2.2.2.2 Biller Isolation

Passwords for Biller Isolation system users are created as part of the installation or modification process using manual scripts.

The password policy should be enforced by the Administrators who created them based on Charter policy.



Note: There is no mechanism to enforce it in Weblogic.

6 Authentication

6.1 Assumptions – N/A

6.2 Solution

Any access to the Amdocs system requires authentication. In this solution, password based authentication will be used, except for third party components as detailed in below.

The following table depicts the mapping between the Amdocs applications in scope of the Charter solution and the authentication provider that authenticates the various types of users attempting to log in to these systems.

Table 2: Authentication Providers Mapping

User Type	Charter's AD	ASM	Local
Back office – Charter Employees (Admin, Business, etc.)	Biller Isolation (web-admin), MEC, Reporting & BI		
Back office – System Users *	MEC	Ordering (BE), REST services	Biller Isolation

* System users, for internal functionality (such as batches and jobs), are maintained in the application repository.

6.2.1 External Authentication

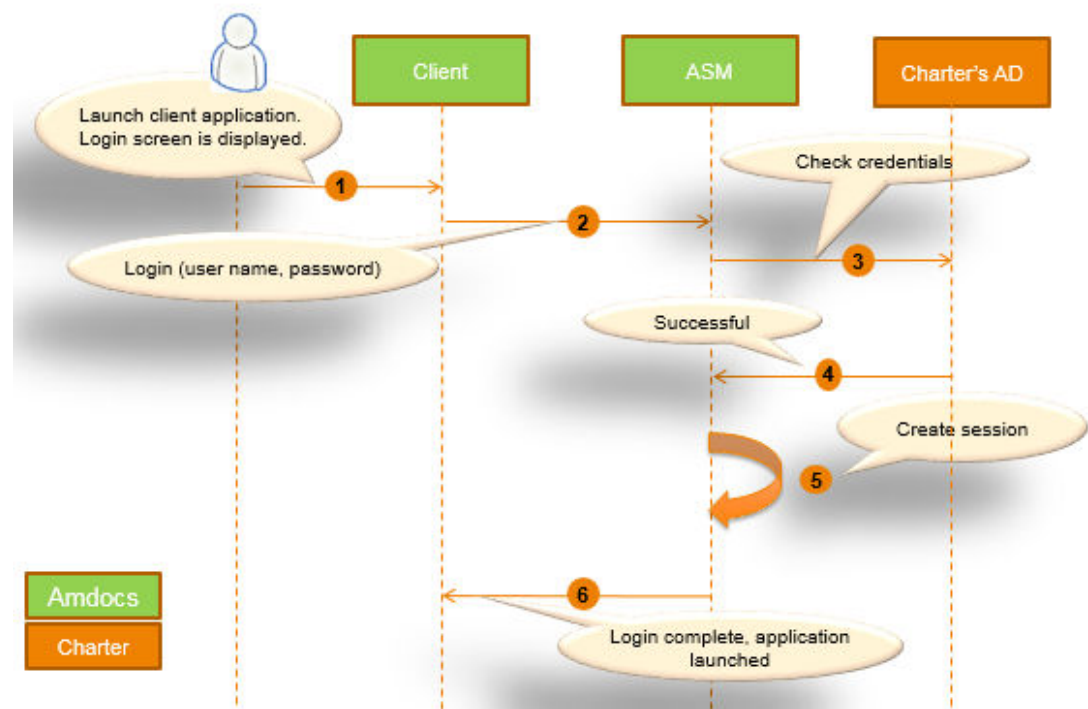
In this solution, external authentication is used for all interactive logins for all applications and MEC back office users, in scope as per the mapping in Table 2.

Authentication against Charter's AD will be done using simple LDAP authentication (user + password) (Microsoft AD over LDAPS V3 protocol).

6.2.1.1 Amdocs Components

Amdocs components listed in section 1.1 Purpose and Scope use ASM as their authentication gateway. Charter employees using the component consoles will be authenticated against Charter Active Directory. The following sequence diagram depicts the external authentication process for these components:

Figure 6-1: External Authentication



Where:

1. The user (Charter employee) launches the relevant application console, and is required to provide his credentials.
2. The credentials are sent from the client application to ASM to perform the login request.
3. ASM delegates the authentication decision to Charter Active Directory, using LDAP's v3 protocol.
4. The authentication response is returned to ASM.
5. Upon successful login, an ASM ticket (session) is generated and stored in ASM repository.
6. The ASM ticket is sent to the client application as proof of authentication.

6.2.1.2 Reporting & BI

Reporting & BI (QlikView) authentication is based on Microsoft Active Directory authentication (Kerberos). In this case, a Charter employee who is already authenticated to work on their workstation opens the Reporting & BI console, will have the Single Sign On (SSO) solution implemented.



Note: QlikView will utilize the authentication provided by the target system when connecting to external resources. Credentials will be kept in the QV encrypted connection string.

6.2.2 Consuming Amdocs Services

Access to the Amdocs system, regardless of the calling source, requires authentication. In this solution, any access to the Amdocs system will be routed via the Charter Gateway, which is responsible for user authentication

The authentication mechanism is based on a single system user (of the calling system). This user is maintained either in an ASM repository or in the local repository of the component (in the case of Biller Isolation). The credentials of this user are expected to be securely stored by the calling application.

6.2.2.1 REST Services

In this solution, REST services will be used for consuming Ordering services.

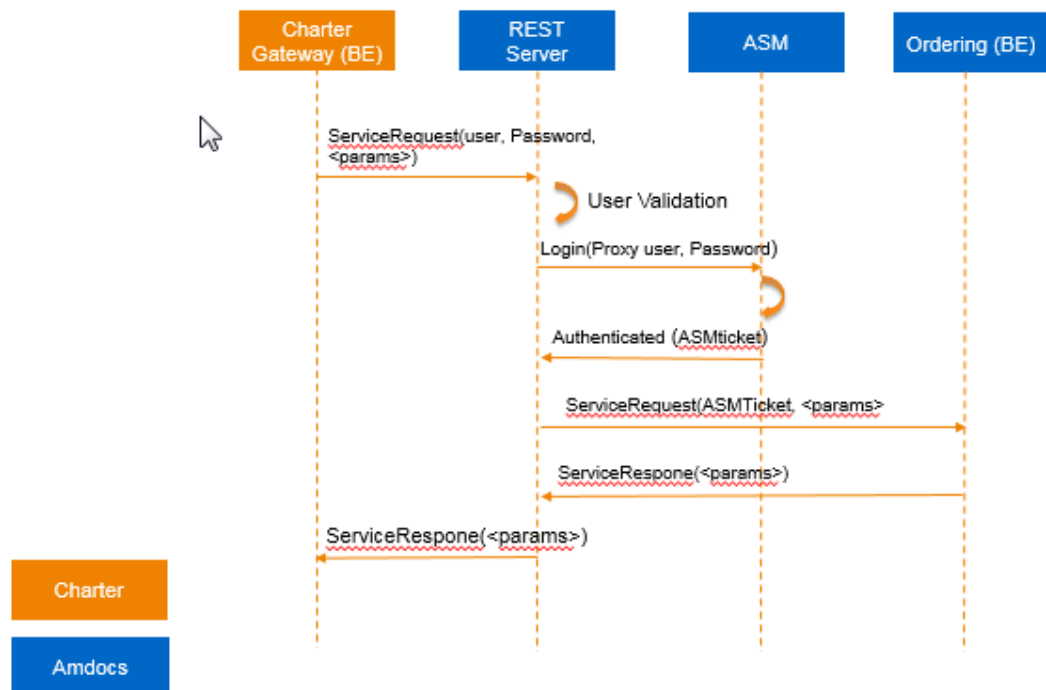
Similar to the entire solution, the REST services authentication solution will be basic authentication to the REST server - that is, a password based authentication, where the Charter Gateway sends the proxy username and password identifying it, in every request.



Note: The originator user's information will be sent by Charter Gateway as part of the REST request (HTML header).

The REST server invokes a pre-defined system user for consuming internal services.

The following diagram depicts at the high level the authentication flow for consuming the REST services.



Where:

1. Charter Gateway sends the service request along with its pre-defined credentials to the REST server.

2. The REST server performs internal authentication/validation of the credentials it received.
3. On successful completion of step 2, the REST server performs an explicit login to the backend ASM (Ordering ASM – please refer to section 5.2) in order to obtain an ASM ticket.
4. ASM authenticates the REST server, generates a session for this user, and returns the ticket (representing the session) to the REST server for successive calls.
5. The REST server sends the service request it got in step 1 to the Ordering backend.
6. Ordering backend performs the service request and returns the response to the REST server.
7. The REST server forwards the response back to Charter Gateway.

6.2.2.2 Biller Isolation Services

The Biller Isolation services will be exposed as Web Services consumed by Charter Gateway. Authentication of these services will be done locally within the Biller Isolation component, and will be done using a system user and password, which will be pre-defined in Biller Isolation in advance.

Biller Isolation supports WS Security standards, and its services are stateless – that is, no session management is provided and every call is re authenticated, so on each call, the Charter Gateway is expected to provide its credentials.

6.2.3 Consuming External Services

Service consumption by the Amdocs system will be done by the Biller Isolation component. This will be done using a pre-defined system user of the Charter Gateway that will be stored in the Biller Isolation database.

The system user password will be stored encrypted using AES 256 algorithm and Tomcat encryption facility, and will be sent on each service request as part of the WS Security notation (SOAP). In other words, all calls are assumed to be stateless.



Note: Target system security is Charter's responsibility.

6.2.4 File Access Authentication

File transfer authentication will be done using the infrastructure security.

Direct access to the database should be restructured to authorized users only.

Some of the Amdocs components, such as MEC, have file interfaces.

File depots and repositories on the disk should be protected using OS security. A system user is defined at the OS level, with limited access rights to the predefined directory only, for downloading or uploading files.

Download from the BSS system is performed from the secure zone only.

Files are transferred to the BSS system using the Secure FTP protocol.

Creation and management of OS users that require access to Amdocs servers is not in the scope of this document.

6.2.5 ASM Session Management

Amdocs Security Manager (ASM) is responsible for session management of Amdocs applications.

A session object is created for every successful user authentication and stored for the duration of the user session. The session object contains various user details, such as the user roles. The session ticket serves as the unique ID for the session in the system; it is a randomly generated string that consists of 40 characters in length, which does not include any user or session details, but only references to these details (session object) in the repository.

The ASM ticket is sent by the client, along with the business parameters, to the server. Before performing any activity, the ASM ticket is verified first on the server side by ASM. Only if the ASM ticket is valid, then the required activity is executed.

The session policy in ASM enables defining the following attributes:

- *User sessions max number* – Indicates the maximum number of simultaneous sessions allowed for the user. A user session is any attempt the same user makes to log in to the system.



Note: The default value is 10.

- *Session expiration time* – The maximum length of a session (in seconds)



Note: The default value is 86,400 seconds (the equivalent of 24 hours).

- *Session idle time* – The maximum idle time allowed (in seconds) before the session is disabled.



Note: The default value is 1,800 seconds (the equivalent of 30 minutes).

The session is refreshed every time an application or a user presents a session ticket. Each time ASM converts an application ticket to an ASM token, the session is refreshed.

There are three cases when a session object or session token can become invalid:

- Logout process
- Session idle timeout
- Session expiration

When a session times out in Amdocs system, the application blocks the user from performing additional activities until re-login occurs.

7 Authorization

7.1 Assumptions

1. Role lists and protected element lists will appear in the HLD of each application and are out of scope for this document.

7.2 Solution

Authorization refers to the controls that govern the resources and operations that an authenticated client is permitted to access.

The access control mechanism in the Amdocs system is Role Based Access Control (RBAC) or Role Based Authorization (RBA), which is checked on the server side.

The organization model is built around what people do, including their level of responsibility, the people they work with, and the business entities (for example, accounts or cases) they work on. In RBAC, these factors are referred to as 'roles'. This can be, for example, CSRs, Managers, Administrators (with/without emergency role authorization set, and so on).

Each user in the Amdocs system must be assigned with at least one role.

The following table summarizes the role management per application along with authorization mechanism used by these systems:

Table 3: Authorization Mapping

Application	Role Declaration & User/Role Linkage	Role Management	Authorization Decision Point
Ordering (BE), REST services	ASM	ASM	ASM
MEC	ASM	ASM	ASM
Biller Isolation – Admin	ASM	ASM	ASM
Biller Isolation – APIs	None	None	Biller Isolation
Reporting & BI	Internal	Internal	Internal

The different authorization mechanisms are detailed in the following sections.

Role management is performed through the administrative consoles of the applications, that is the ASM security console or the Reporting & BI console, for authorized users only (typically, security administrators).

Role implementation is business driven and should be done based on the 'Need to Know' concept in order to achieve segregation of duties and to assign the minimum required permissions set for performing their tasks.

A prerequisite step to role implementation is role engineering. During the BPT phase, Amdocs and Charter will work together to define the needed roles in the system. The output of this process will be mapping of the defined roles in the system.

7.2.1 Amdocs Security Manager

Amdocs Security Manager provides an authorization service that acts as a decision point for calling applications. An application calls Amdocs Security Manager to check whether a user has access to a specific resource and acts accordingly.

When creating a session (after a successful login), ASM builds the user's security profile.

In order to provide a flexible and powerful authorization mechanism, ASM offers an authorization scheme that is based on protecting resources, with policies that contain authorization rules.

A *resource* is an application-protected element, such as an API, a file, an event, or a GUI control. A protected *resource* is a basic item that can have access control. This means that an application can perform the authorization check before access or usage of the resource.

Resources are used mainly for activities that are carried out in EJB-type client applications. Each resource is mapped to a specific EJB resource – an interface or a method – for example, resources such as getAddress, getCustomerInfo, makePayment, and so on.

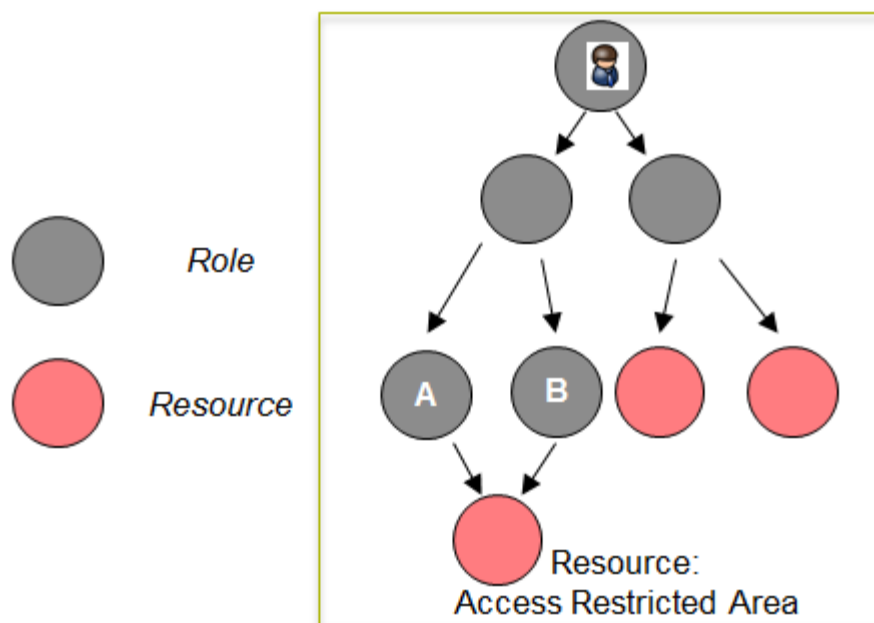


Note: Resources are created by the development team and automatically imported.

A *role* is a set of predefined access permissions to resources that can be granted to a specific user. The Security Administrator assigns roles to users (alternatively, the IAM system can provision users with “roles”), which determine their access rights. Roles can be organized in a role hierarchy, and one role can contain another role, which in such a scenario, all sub-roles and their sub-roles and all resources that are assigned to them are authorized for the assigned user.

The following diagram illustrates the role hierarchy in ASM:

Figure 7-1: Amdocs Security Manager Role Hierarchy



7.2.2 Biller Isolation APIs

The authorization decision of the Biller Isolation services (APIs) is done internally by the components, as per the system user definitions.

7.2.3 Monitoring & BI

All authorizations will be based on the internal definitions in the application.

Permissions will be assigned to Active Directory defined users.

Administrative access will use the same authorization solution.

7.2.4 MEC



MEC is based on ASM authorization. This determines what a user is allowed to perform when access to the system is obtained. The authorization is performed using roles, which enable granting/denying access to view items, projects, query results, validation results, auditing information, and element views.

A user can have more than one role simultaneously. In such cases, the least restrictive set of permissions takes precedence.

7.2.4.1 Managing Permissions for Roles

After users and roles have been defined in the system using the ASM console application, permissions for the roles using MEC must be set.

In contrast to users and roles, the actual access permissions for each role are managed in MEC itself. There is a built-in system role, EPCAdmin, which grants administrators access rights and allows defining sets of access permissions.

Item Types and Operations	Description
Item types	
Elements	View, create, and modify elements.
Elementary Types	View, create, and modify elementary types.
Queries	<p>View, create, modify, and execute queries. If you set the permission for queries to Read Only, the user cannot execute queries.</p> <p> <i>Note: To enable viewing the results of queries, grant permission for viewing elements must be defined.</i></p>
Projects	<p>View, create, open, close, and validate projects and modify project properties. Read Only permissions means that the user can only open and close a project.</p>
Templates	<p>View, create, and modify templates. You can define specific permissions for templates and elements that are created from the templates using the template user access.</p>
Element-View Definitions	<p>View, create, and modify element view definitions. You can define specific permissions for the element views that the element view definition defines.</p>
Operations	
Export	Export data from Enterprise Product Catalog.
Import	Import data into Enterprise Product Catalog.
Role Definition	<p>Define permissions for roles.</p> <p> <i>Note: Caution: If you deny permissions to Role Definition from the user role with which you are logged in, you will no longer be able to manage role definitions.</i></p>
Full Distribution	Distribute all items in the Enterprise Product Catalog database with the status of 'Released'.
Project Supervisor	Define the project supervisor.
Item Modification	Create new items and check out existing ones
Element Versioning	Add and modify element versions
Element Versioning-Backdating	Modify the dates of previous versions
Template User Access	<p>Configure the template user access, which defines specific permissions for templates and elements that are created from the templates. To enable access to the template user access, you must grant permissions to the Template item type.</p>
Change Project Status	Manually change the project status.
Get Distribution Results	Retrieve the distribution file using external services.

View Auditing Info	Display auditing information.
Elements Default View	View and modify the default elements view.
Catalog Versioning Modification	Create or delete a catalog version, change a version description, and change the planned production date of the catalog version.
Change Catalog Version Status	Change the status of the catalog version.

For each role, the permissions must be specified explicitly; otherwise, the user granted the role is unable to manage certain resources or perform necessary operations.

In addition to the EPCAdmin role, there is another predefined MEC role, Implementer, which gives full access to MEC and its item types only.

The following table describes the operations and item types for which permissions can be defined on the Role Definition screen.

7.2.4.2 Enterprise Product Catalog Role Definitions:

The OOB configured permissions are:

- *Full Access* – the role that this permission is associated with is allowed to view and modify the item type.
- *Read Only* – the role that this permission is associated with is allowed only to view the item type. No other actions, such as modify, are allowed for this role.

7.2.4.3 Managing Access to Elements

Access to elements and element views can be limited to specified users only. In addition, the security administrator can define which elements users can view and the order and organization in which the elements appear.

The following access rights can be defined:

- Access for viewing the default element view, which displays the elements based on the template from which they were created. To define the access to the default element view, define the permissions for the Elements Default View property in the Role Definition.
- Create element views that display elements in a specified order. It is possible to define which elements to display and the order in which they appear. To define a new element view, the user creates element view definitions.

7.2.4.4 Managing Access to Templates

MEC enables the security administrator to define user access rights for views and definitions of the template and the elements that are created from the template. By defining template user access, the security administrator is able to define a more granular definition than the user access rights than can be defined using the role definition.



Note: You must grant the role access rights for templates and template user access in the role definition or the template user access will be ignored.

8 Audit

8.1 Assumptions – N/A

8.2 Solution

Security-relevant events are collected by each security framework used by the different components.

The following table maps the different components and the security framework responsible for the security auditing.

Application	Security Auditing Framework
Ordering (BE), REST services, MEC, Biller Isolation - Admin	ASM
Biller Isolation – APIs	Internal
Reporting & BI	Microsoft windows server and the IIS capabilities

The following sections detail the security audit capabilities.



Note: Functional/business auditing is handled by the applications themselves, and are not covered in this document.

8.2.1 ASM

Security-relevant events, including security administration events that are performed by ASM, are logged by ASM, even if they are also logged at other system levels.

For each event record, the following information is logged:

- Date and time of the event
- User ID
- Event type
- Success or failure status of the operation (both for authentication failures and successful log-in processes)
- Facility (log host name, application name, and module) generating the event record. This is recorded to aid in merging multiple log streams.

Security-relevant events and their attributes include:

- *Session initiation (log-in process)* – Includes user identity and authentication activities (login/logout), as well as the success or failure of the log-in process
- *Session termination (log-out process)* – Includes the following possible reasons:
 - User request
 - Timeout
 - Operator intervention

- *Account Management Operations* – Each access (read and write) to the account databases (on the application server) is logged, in the same way as the other requirements.
- *System Start-up/Shutdown* – Includes the following reasons:
 - Automatic
 - Operator intervention
 - Fault

Audit logs in ASM are maintained in the database and are configurable.

8.2.2 Biller Isolation – APIs

Biller Isolation APIs, i.e., the web-services, enable auditing with the following fields.

- **GTXID**: global transaction ID
- **TXID**: unique transaction ID
- **StartDate**: date of request (in milliseconds)
- **EndDate**: date of response (in milliseconds)
- **ServiceName**: operationName
- **ModuleName**: EG/Channel name
- **SourceSystem**: USER_IP_ADDRESS
- **TargetSystem**: external target system name
- **Status**: service status number (for example, 200)
- **HandlingTime**: TOTAL_SERVER_TIME in milliseconds (endDate-startDate)
- **ErrorCode**: Service error code
- **Description**: Service error description
- **EntityID**: orderID/CustomerID

8.2.3 Monitoring & BI

As Monitoring & BI relies on Microsoft Active Directory services, its auditing is based on Microsoft Windows server and the IIS capabilities.

Every access is logged, and the Active Directory account of the user is kept at the system level.

9 Confidentiality

9.1 Assumptions – N/A

9.2 Solution

Confidentiality refers to protection of sensitive information through implementation of appropriate controls.

In the Charter solution, the following table describes the attribute considered to be sensitive:

Sensitive Data:

Table 9-1: Sensitive information mapping

Field Type	Acceptable for Storage	Encrypt/Hash If Stored	Mask on Display	Scramble in QA/Dev	Field Level Logging	Referenced Applications
Passwords	Yes	Yes (Hashed/Encrypted)	Yes	Yes	Yes	ASM, All

9.2.1 Sensitive Data at Rest

Sensitive data at rest (as per table 9-1 above) that is stored in Amdocs's repositories, are protected as follows::

- Use passwords stored in ASM and Biller Isolation databases are hashed using the SHA-2 algorithm.
- Passwords in configured files and databases are encrypted by the application using standard algorithms.



Note: Where technically not possible, strict ACLs (Access Control Lists) are defined for property files containing passwords for the purpose of preventing unauthorized access.

9.2.2 Sensitive Data in Transit

Sensitive information in transit is sent over the public network using HTTPS (SSLv3).

9.2.3 Masking Sensitive Data on Display

Sensitive data is masked on display as explained in the Sensitive Data table above.

9.2.4 Masking Sensitive Data in Logs

Sensitive data (as per the definition in the Sensitive Data table above) is masked or truncated in logs.

10 Infrastructure Security

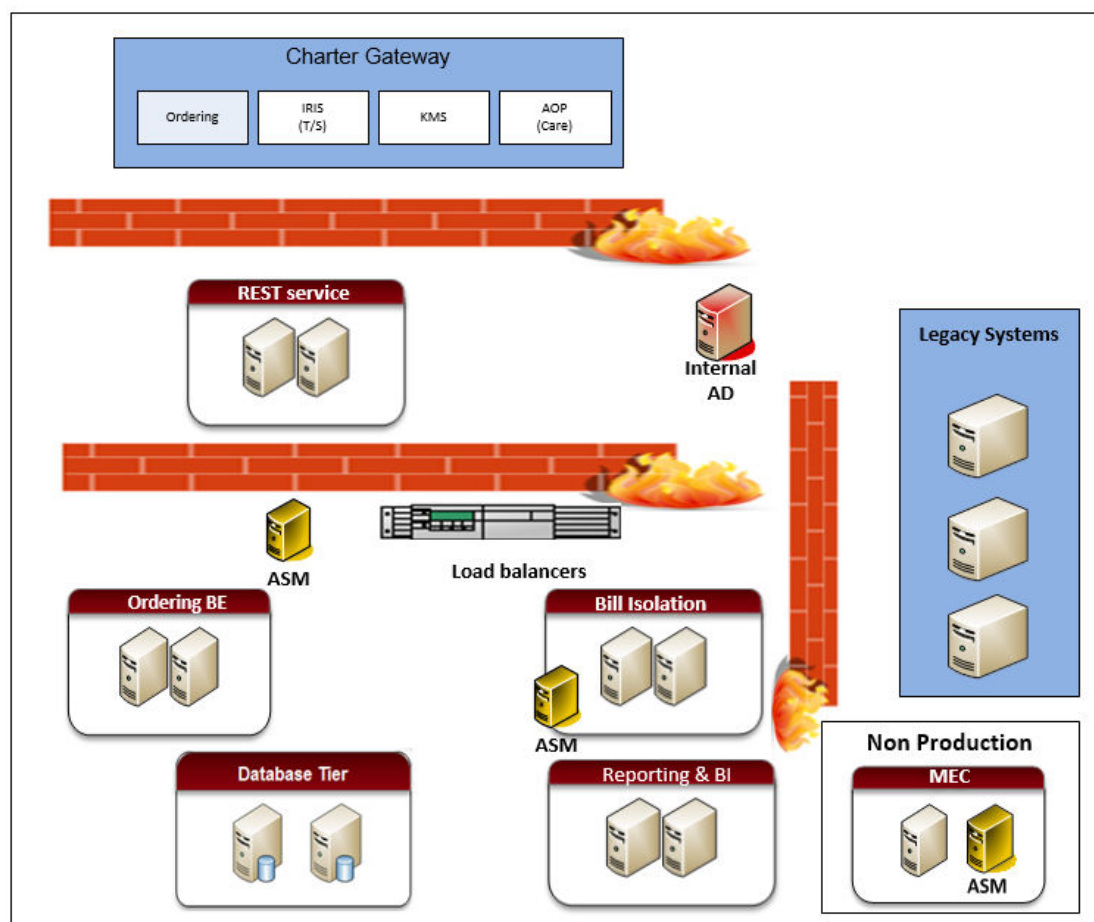
In the Charter project, infrastructure security, like installation, configuration, and operations of the network, remote access, servers, databases, operating systems, and third party appliances, is Charter's responsibility. The following sections detail Amdocs best practices for infrastructure security of its system deployment.

10.1 Network Design

10.1.1 Assumptions – N/A

10.1.2 Solution

Separated security zones in multi-tier access design



The multi-tiers security zones solution depicted in the diagram above was created taking into account the following considerations:

- Filtering device awareness and standard protocol use, allowing FW separation
- Separate environments for production and non-production

- Separate administration networks can be supported for Out of Band (OOB) administration, system high availability, audit, and so on.

10.2 Users and Privilege Management

10.2.1 Assumptions – N/A

10.2.2 Solution

10.2.2.1 System users

- Charter will manages all users on the operating system level.
- Privileges are defined by Charter and enforced by them.
- Password policy is enforced in accordance to Charter policy.
- Amdocs users will be granted only the required permissions to be able to perform their work.
- No root user is required by default and, if needed, the user will ask for specific privileges add hoc.

10.2.2.2 Application/service accounts

- Dedicated users are used per application and service only.
- No use of the root user.
- Users are granted with the minimum of needed privileges.
- Users will be defined and granted a password as part of the installation by Charter.

10.2.2.3 Database accounts

- Database accounts are managed by Charter.
- No DBA permissions should be in use except for management tasks.
- Dedicated users are used per application or service.
- Users are granted with the minimum of needed privileges.

10.3 Logging and Auditing

10.3.1 Assumptions – N/A

10.3.2 Solution

Amdocs utilizes Audit to allow traceability, accountability, and forensics.

- Infrastructure audit is performed based on:
 - The component's audit capabilities
 - Performance considerations
 - Business needs
- Operating system audit can be utilized for logging all events. Per Amdocs best practices, the audit can be set to LogLevel INFO

- Database Audit - Amdocs best practices considering performance and sizing is to enable Audit of administrative users only.
- Operating system and database Audit information can be sent to a central Syslog facility.
- Audit logs can be collected by a SIEM solution.
- Log rotation and retention should be configured per component and according to its storage restrictions.
- Reporting and investigating can be done on the central SIEM or by direct access to system logs.
- Additional logging can be achieved by adding specific security tools (DBF, IDS/IPS, FIP).

10.4 Access Management and Data Protection

10.4.1 Assumptions – N/A

10.4.2 Solution

- Access to the system can be limited using standard FWs.
- Amdocs utilizes standard protocols and allows opening only the needed ports.
- FW systems should be capable of processing the traffic, and correct planning will prevent degradation on performance.
- Other security tools, like DBF, IDS and others, can be utilized; however each tool must be aligned with the system performance SLA and should not add latency above the system limit.
- Data at transport is protected using secured protocols:
 - SSH, SFTP are utilized on the Infrastructure level.
 - SSL is utilized for public access (Internet).
 - Internal SSL can be utilized until the load balancers.
 - LDAPS is used to integrate with the LDAP service.
- Data at rest can be protected.
 - Passwords are stored hashed or encrypted by the relevant component.
 - Where technically not possible, ACLs will be used to protect against unauthorized access.
 - Backup should be encrypted by the backup application.
 - Non-production data should be scrambled or masked.
 - Restricted ACLs are implemented on the file store.

Appendix A Amdocs ISO 27001 Certificate

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

IQNet and
THE STANDARDS INSTITUTION OF ISRAEL
hereby certify that the organization

AMDOCS LTD.

WORLDWIDE

for the following field of activities

IT SYSTEMS, MANAGED SERVICES, GLOBAL SOURCING,

SOFTWARE DEVELOPMENT, PRODUCT SECURITY

MANAGEMENT AND INTELLECTUAL PROPERTY (IP)

PROTECTION.

has implemented and maintains a

Information Security Management System

which fulfills the requirements of the following standard/s

SI ISO 27001:2005

Issued on : 29 . 09 . 2014

Date of expiration: 28 . 09 . 2017

Date of initial approval: 14 . 07 . 2005

Registration number:

IL-43805




Michael Drechsel


Daniel Goldstein



Document Release Information

SW Ver.	Editor/Author	Application	Edit Date [Mmm-dd-yyyy]	Section	Changes	Sent to site	Approving Manager	DC Ver.
	Mazal Shelli				Initial version	N		0.1
					Template conversion and initial TW review	N		0.2
						Y/N		
						Y/N		
						Y/N		
						Y/N		