ISEC7 SPHERE
SUPPLEMENTAL PROCEDURES

Version 2, Release 1

23 October 2020

Developed by ISEC7 and DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

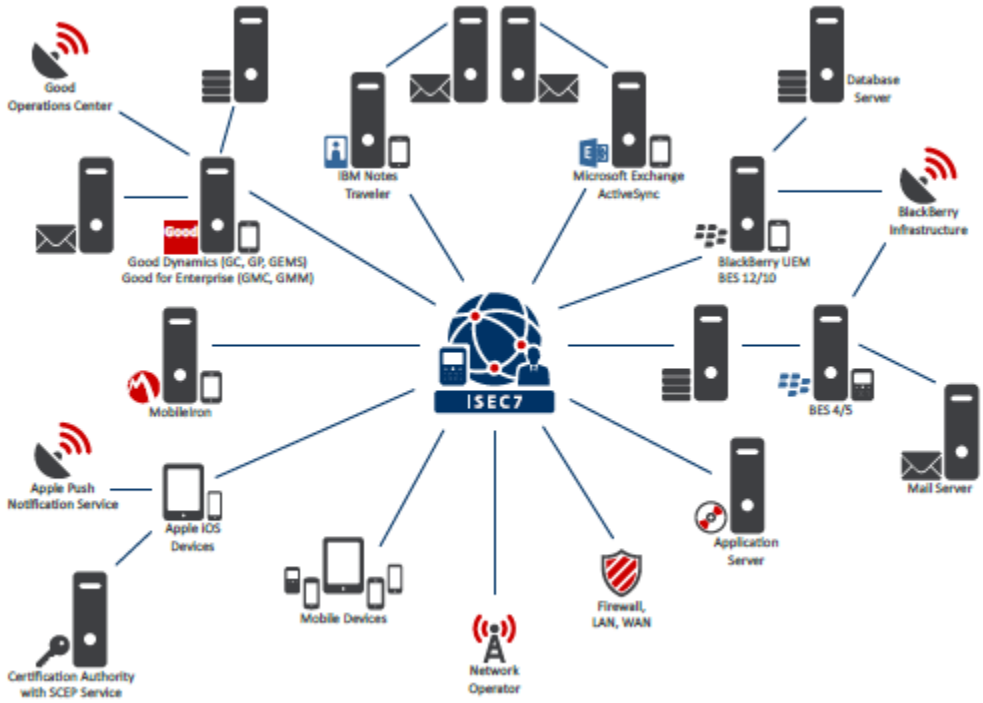
LIST OF FIGURES

Page

1. ISEC7 SPHERE SECURITY AND CONFIGURATION INFORMATION

1.1 Architecture

Figure 1-1: ISEC7 Sphere Architecture



Note: ISEC7 Sphere was formally called ISEC7 EMM Suite. The previous name may be found throughout this STIG.

1.1.1 Network Configuration

ISEC7 Sphere collects data from all relevant mobile infrastructure components and stores the compressed data in a SQL database. ISEC7 Sphere uses technologies such as Web Services, SNMP, WMI, DIIOP, PowerShell, network diagnostics tools, databases parsing, and log files to obtain data remotely from servers or via ISEC7 Sphere Agents located directly on a monitored system.

Table 1-1: Outbound Ports

Source	Target	Protocols	Default Ports	*
Monitor	https://license.isec7.com/	HTTP/S	80 / 443 / Proxy	1

Table 1-2: Listening Ports

Source	Target	Protocols	Default Ports	*
Any	ISEC7 EMM Suite web application	HTTPS	443	
Monitor	ISEC7 EMM Suite Database	TSQL / SSL	1433	
Monitor	ISEC7 EMM Suite Database Server	UDP	1434	5
Monitor	AD/LDAP/GC	LDAP/SSL	389/636 / 3268/3269	
Monitor	DNS Servers	DNS	53	1
Monitor	SMTP Gateway	SMTP/SSL	25 / 465	
Agents	Monitor	TCP/IP	13657	
Agents	Web/Monitor	HTTP	8080	
Monitor	Hosts Monitored via SNMP	SNMP	161 (UDP)	1
Monitor	Ping monitored systems	ICMP/TCP	any	6
Agent	Ping monitored systems	ICMP/TCP	any	6
Agent	Network shares	SMB	445	1
Agent	Hosts monitored via WMI	DCOM/WMI	135 / any	
Monitor	Monitored web servers	HTTP/S	80 / 443 / any	
Monitor	BES12/UEM Web Services	HTTPS	18084	
Monitor	UEM Database	TSQL/SSL	1433	4
UEM Core	Monitor	SNMP (Trap)	1620 (UDP)	
Monitor	BES10 Web Services for BDS	HTTPS	38443	
Monitor	BES10 Web Services for UDS	HTTPS	18082	
Monitor	BlackBerry Servers	SNMP	161	1
Monitor	BES4/5 Management Databases	TSQL/SSL	1433	
Agents	BES4/5 Management Databases	TSQL/SSL	1433	2
Monitor	BES4/5 Mobile Data Services	HTTP	8080	
BES4/5 MDS	Web/Monitor	HTTP/S	8080 / 443	
Monitor	Good Dynamics Web Services	HTTPS	443	
Monitor	Good Mobile Control Web Services	HTTPS	19005	
Monitor	MobileIron Web Service (Core)	HTTPS	443	
Monitor	MobileIron Core and Sentry Servers	SNMP	161	1
Monitor	AirWatch REST API	HTTPS	443	1
Monitor	AirWatch Servers	SNMP	161	1
Agents (local)	Internet Information Servers (IIS)	HTTP/S	80 / 443	3
Monitor	Microsoft Exchange Server 2013+	HTTPS	443	
Monitor	IBM Domino Servers	DIIOP	63148	
Monitor	IBM Domino Servers	HTTP	80	
Monitor	IBM Domino Servers	SNMP 161	1	
Monitor	CA with SCEP Server (RA)	HTTP/S	80 / 443	
Monitor	gateway.push.apple.com	TCP/SSL	2195	1
Monitor	feedback.push.apple.com	TCP/SSL	2196	1
Monitor	APNS 17.0.0.0/8	TCP/SSL	2195 2196	1
Apple iOS Devices	APNS 17.0.0.0/8	TCP	5223	1

Source	Target	Protocols	Default Ports	*
Apple iOS Devices	Web/Monitor	HTTPS	443	
Apple iOS Devices	SCEP Server Web Service	HTTPS	443	

*** Legend:**
1 Not configurable.
2 Only if SQL tunneling from the 'ISEC7 EMM Suite Monitor' through the 'ISEC7 EMM Suite Agent' is used.
3 Only for Microsoft Exchange 2003 ActiveSync monitoring.
4 Only for additional BlackBerry Dynamics monitoring.
5 Only when accessing the ISEC7 EMM Suite database using the SQL Server instance name.
6 Any TCP port used to ping the corresponding host; could be individual for each.

1.2 Identification and Authentication

1.2.1 Passwords

Authentication to ISEC7 Sphere can be configured to use local authentication or an enterprise authentication mechanism, such as Active Directory. The STIG requires that Sphere administrators use Active Directory managed authentication. Management and protection of local server accounts and their access, as well as enforcement of required password rules and policies, is managed by the host operating system. When logging on to the Sphere console, passwords are obfuscated. The STIG requires the Sphere console to be configured to use an enterprise authentication mechanism.

Negotiated keys/passwords are negotiated through established and approved key agreement schemes using FIPS-validated cryptographic modules. All communication between agents/clients and ISEC7 Sphere is encrypted.

1.2.2 Certificates

Management of certificates on the server hosting ISEC7 Sphere, including verification, validation, and protection is the responsibility of the host operating system.

A DoD PKI-issued certificate must be used during the installation of ISEC7 Sphere. If a self-signed certificate was used during server installation, it must be replaced with a DoD PKI-issued certificate.

1.3 Maintenance

Access management and control for nonlocal maintenance and diagnostic sessions is managed by the host operating system and is out of scope for ISEC7 Sphere.

1.4 Media Protection

Access to and control of removable media and other storage used by ISEC7 Sphere is managed by the host operating system.

1.5 System and Communication Protection

1.5.1 System Protection

Protection of ISEC7 Sphere and any storage of data used by and/or created by the ISEC7 Sphere are managed by the host operating system. This includes storage and protection of any keys, certificates, and/or protected classified information.

2. OPERATIONAL CONSIDERATIONS

2.1 Monitoring and Administration of Mobile Device Management (MDM) servers in the DoD Environment

2.1.1 General

In the DoD environment, mobile devices that store or process sensitive DoD information must be configured to support either a work-only processing environment where no personal applications or data are installed, or configured to support two processing environments: one for work applications and data and one for personal applications and data. When work and personal processing environments are used, personal applications must not be able to access work data. The Mobile Device Fundamentals Protection Profile (MDFPP) defines technical requirements for data separation between the work and personal processing environments.

ISEC7 Sphere supports a broad range of MDMs with the capability to leverage configurations on the MDM, and grant the First Level Support Teams the ability to perform basic administration from the ISEC7 Sphere. These capabilities are provided through Application Programming Interfaces (APIs) provided by the MDMs. All actual administration is performed by the MDM. ISEC7 Sphere provides an interface that allows First Level Administrators with the proper permissions to affect the administration from the ISEC7 Sphere console.

DoD deployed commercial MDM solutions support a broad range of technologies and activation types that provide data separation features compliant with the MDFPP, including iOS-managed and -unmanaged apps, Samsung Knox, and Android for Work. DISA developed operating system STIGs are MDM product independent and therefore do not contain MDM-specific configuration and activation type information. The DISA-developed STIGs for the specific MDMs and mobile devices should be referenced for any configuration questions.

2.1.2 Remote Agent Permissions

ISEC7 Sphere provides an agent to be installed on the local system in order to provide monitoring data to the ISEC7 Sphere solution. In some cases, installing an agent on the local system is not feasible. In these cases, a Remote Agent can be used to allow the ISEC7 Sphere to continue to perform monitoring capabilities to systems without the requirement of installing software locally. When this option is chosen, specific permissions are required based on the monitoring function being performed by the remote agent, which are not included in the standard documentation, as local installation of the agent is preferred.

2.1.2.1 Remote Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification. Remote WMI is the ability to manage and access WMI data on remote computers. In this instance, ISEC7 Sphere uses Remote WMI to

allow an Agent installed on a different system to connect to another server remotely and gather monitoring information.

A service account is added to ISEC7 Sphere and granted the following permissions and group memberships on the system to be monitored.

- Member of the local group "Distributed COM Users"
- Member of the local group "Performance Monitor Users"
- Have "Remote Enable" WMI Control (wmimgmt.msc) permission set on Root/CIMV2 namespace and sub namespaces

2.1.2.2 ActiveSync Log Parsing

ISEC7 Sphere can monitor and identify ActiveSync relationships and statistics from Microsoft Exchange On-Premises installations. Normally, the locally installed ISEC7 Agent would provide the information gathered to the ISEC7 Sphere server, however in some cases, this data is gathered through a remote agent running as a service account configured in the ISEC7 Sphere console. To see device information associated with users, the service account must be issued read access to the portions of the user account details that contain this information. This is accomplished by performing the following for the service account:

- Member of the Active Directory group “View-Only Organization Management”
- Have the “View-Only Organization Management” group added to any OU that contains user accounts and grant it Read access
- Verify permissions are applied to “This object and all descendant objects”