

UNCLASSIFIED



MICROSOFT (MS) EXCHANGE SERVER 2013 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

25 July 2016

Developed by Microsoft and DISA for the DoD

UNCLASSIFIED

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
1. INTRODUCTION.....	1
1.1 Executive Summary	1
1.2 Authority	1
1.3 Vulnerability Severity Category Code Definitions	1
1.4 STIG Distribution.....	2
1.5 Document Revisions	2
1.6 Other Considerations	2
1.7 Product Approval Disclaimer.....	3
2. ASSESSMENT CONSIDERATIONS.....	4
2.1 Security Assessment Information	4
2.2 Exchange Management Shell	4
2.3 Pre-Review Procedure.....	4
2.3.1 Email Domain Security Plan	4
2.3.2 Email Domain Servers and Settings	5
2.4 SRR Method.....	6
3. TECHNOLOGY OVERVIEW.....	7
3.1 Introduction	7
3.2 Exchange 2013 Server Roles	9
3.2.1 Client Access Role.....	9
3.2.2 Mailbox Server Role.....	9
3.2.3 Edge Transfer Server Role.....	10
3.2.4 Email Services Policy STIG	10
3.3 Email Data Overview	10
3.4 Message Access Path	11
3.5 Message Transport Path	12
4. REFERENCE DOCUMENTS	14
5. CONCEPTS AND TERMINOLOGY CONVENTIONS	15
5.1 Operational View	15

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2
Table 4-1: Reference Documentation	14

LIST OF FIGURES

	Page
Figure 3-1: Microsoft Exchange 2013 Architecture Overview	8
Figure 3-2: Message Access Path	12
Figure 3-3: Message Transport Path	13

1. INTRODUCTION

1.1 Executive Summary

The Microsoft Exchange 2013 Server Security Technical Implementation Guides, Edge Transport, Client Access, Mailbox, and Email Services Policy, are published as tools to improve the security of Department of Defense (DoD) information systems. These documents are meant for use in conjunction with the Windows Operating System (OS) STIG and any appropriate STIG(s) applicable to the system.

There are four STIGS available for MS Exchange Server 2013:

- Exchange 2013 Mailbox Server STIG
- Exchange 2013 Client Access Server STIG
- Exchange 2013 Edge Transport Server STIG
- Email Services Policy STIG

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that “all IT that receives, processes, stores, displays, or transmits DoD information will be [...] configured [...] consistent with applicable DoD cybersecurity policies, standards, and architectures” and tasks that Defense Information Systems Agency (DISA) “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is <http://iase.disa.mil/>.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to the protect vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<http://www.niap-ccevs.org/>) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<http://csrc.nist.gov/groups/STM/cmvp/>) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (<http://www.disa.mil/network-services/ucco>) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

The MS Exchange Server 2013 Security Readiness Review (SRR) ensures the site has properly provisioned and implemented the application and it is being managed in a way that is secure, efficient, and effective. The STIG identifies vulnerabilities that undermine security, in that they have the potential to affect the confidentiality, integrity, or availability of email services. The items reviewed are based on standards and practices published by the DoD, its contractors, and other security guidance entities, following guidance published in the Department of Defense Instruction (DoDI) 8500.2 and National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 security controls.

DISA has assigned a level of urgency to each finding based on Chief Information Officer (CIO) established criteria for Certification and Accreditation (C&A). All findings are based on regulations and guidelines. All findings require correction by the host organization.

2.2 Exchange Management Shell

The Exchange Management Shell, built on the Windows Power Shell technology, provides a powerful command-line interface for MS Exchange Server 2013 that enables automation of administrative tasks. With the Shell, you can manage most aspects of Exchange. Several checks and fixes in the STIG are only available through the use of the cmdlets.

Open the Exchange Management Shell and complete the following steps:

Click Start >> All Programs >> Microsoft Exchange Server 2013
Click Exchange Management Shell

Note: The Windows Power Shell is also used to perform several Operating System (OS) and Internet Information Services (IIS)/Client Access (CA) checks.

2.3 Pre-Review Procedure

2.3.1 Email Domain Security Plan

It is a best practice and a DoD requirement for systems to have a documented security plan. Because there are additional, unique system attributes that pertain to email applications, a separate plan-within-a-plan is recommended and is referred to as the Email Domain Security Plan (EDSP). Email domains are entities whose configurations not only affect internal system behaviors but also interaction between email domains. Settings such as certificate names for authentication, mailbox size quotas, or partner domain interaction can be unique for sites. Also, depending on domain size and network type, certain tuning parameters must be set optimally to ensure reliable message throughput.

The Exchange STIG requires that these values be deliberately set and documented to confirm the system is configured as engineered. Obtaining the email system configuration specifics as identified in the EDSP will aid the reviewer in comparing values set to values documented.

The National Institute of Standards and Technology (NIST) Special Publications (SP) in the 800 series are of general interest to the computer security community. This series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations. The NIST 800 series Special Publications can be referenced at: <http://csrc.nist.gov/publications/PubsSPs.html>.

NIST publication SP800-53, which is publicly available, is titled "Security and Privacy Controls for Federal Information Systems and Organizations". The SP800-53 provides information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

NIST publication SP800-18, which is publicly available, is titled "Guide for Developing Security Plans for Federal Information Systems". The SP800-18 provides both guidelines and a template for security plan creation and can serve as a base for development.

NIST publication SP800-45, which is publicly available, is titled "Guidelines on Electronic Mail Security". The SP800-45 provides both guidelines and a template for security plan creation and can serve as a base for development.

2.3.2 Email Domain Servers and Settings

The following commands will provide the exchange environment information that will be needed to perform a review. The reviewer will be able to determine the roles of each server that is configured to perform and determine if servers are providing multiple roles. The exchange environment could consist of 2 servers or as many as 20 in a large enterprise. The commands can be piped to a text file for reference during the review.

```
Get-ExchangeServer | Format-List Name, ServerRole Get-MailboxServer | Format-List  
Name, Identity  
Get-TransportConfig | Format-List
```

To pipe the results to a file, use the following command:

```
Get-TransportConfig | Format-List >> c:\temp\filename.txt
```

Note: The cmdlets are not case sensitive. They may be entered in upper-case, lower-case, or any combination of both to return results. The commands are written to make the command more intuitive by using upper- and lower-case characters.

2.4 SRR Method

To perform a successful SRR, this document and accompanying STIGs provide the methods to assess vulnerabilities on deployed MS Exchange servers. The review process is manual.

3. TECHNOLOGY OVERVIEW

3.1 Introduction

MS Exchange 2013 introduced a number of architectural and fundamental changes compared to Exchange 2010. Instead of the five server roles that were present in Exchange 2010, in Exchange 2013, the number of server roles has been reduced to three: the Client Access server, the Mailbox server, and with Exchange 2013 Service Pack 1, the Edge Transport Server role.

In Exchange 2013 the Client Access and Mailbox roles host the services previously handled by the Hub Transport, Client Access, Mailbox, and Unified Messaging Roles. The hub transport role from 2010 is now split between the Client Access Server and Mailbox Server roles. The Unified Messaging role from 2010 is now combined into both Mailbox and CAS roles.

Another change is the management console interface. The Exchange Admin Center (EAC) is a web-based, all-in-one management console that replaces the Exchange 2010 Exchange Management Console (EMC) and the Exchange Control Panel (ECP), Public Folder Administration Console, Role-Based Access Control (RBAC) User Editor, and Unified Messaging.

[https://technet.microsoft.com/en-us/library/JJ150540\(v=EXCHG.150\).aspx](https://technet.microsoft.com/en-us/library/JJ150540(v=EXCHG.150).aspx)

MS Exchange Server 2013 is a 64-bit email application currently licensed and distributed to the DoD by the Microsoft Corporation and is compatible with MS Windows 2008 Server SP2 or newer.

[illegible]

3.2 Exchange 2013 Server Roles

3.2.1 Client Access Role

The Client Access Server role is the server that clients (e.g., Outlook, Outlook Web App, ActiveSync) connect to for mailbox access. The Client Access server authenticates and redirects or proxies those requests to the appropriate Mailbox server. There are two main components: Client Access service and Front End Transport service.

The Client Access service performs the following functions:

- Provides a unified namespace, authentication, and network security
- Handles all client requests for Exchange
- Routes requests to the correct Mailbox server
- Proxies or redirects client requests for legacy servers, such as Exchange 2007 and Exchange 2010 Client Access
- Enables the use of layer 4 (TCP affinity) routing

The Front End Transport service:

- Runs on all Client Access servers and acts as a stateless proxy for all inbound and outbound external SMTP traffic
- Does not inspect message content but can filter messages based on connections, domains, senders, and recipients
- Only communicates with the Hub Transport service on a Mailbox server and does not queue any messages locally

3.2.2 Mailbox Server Role

The Mailbox Server role stores mailbox data. Mailbox servers can be organized into back-end clusters that use Database Availability Groups (DAGs).

Mailbox servers house the mailbox data for the organization and perform data rendering and other operations. Mailbox servers can be grouped into back-end clusters that consist of database availability groups. The Mailbox servers perform the following functions:

- Host mailbox databases
- Provide email storage
- Host public folder databases
- Calculate email address policies
- Conduct multi-mailbox searches
- Provide high availability and site resiliency
- Provide messaging records management and retention policies
- Handle connectivity because clients do not connect directly to the Mailbox servers

- Provide all core Exchange functionality for a given mailbox where that mailbox's database is currently activated
- Fails over mailbox access when a database fails over

The Mailbox server also runs two Transport services:

- Hub Transport service – Similar to the Exchange 2007/2010 Hub Transport Server role, this service provides email routing within the organization, and connectivity between the Front End Transport service and the Mailbox Transport service.
- Mailbox Transport service – This service passes email messages between the Hub Transport service and the Mailbox database.

3.2.3 Edge Transfer Server Role

Edge Transfer servers are designed to sit in a Demilitarized Zone (DMZ) network to provide Simple Mail Transfer Protocol (SMTP) connectivity and mail flow in and out of the organization. The Edge Transport Server role minimizes the attack surface and handles all Internet-facing mail flow, providing SMTP relay and smart host services for the Exchange organization.

The Edge Transport Server role, as the first point of contact for inbound message batches, owns the task of performing tasks, such as Sender Authentication, spam evaluation, enabling attachment stripping policies, archiving filtered messages, logging activity results, and alerting administrators to findings. The Exchange Edge Transport Server guidance must be used when MS Exchange is deployed in the Edge Transport Server role.

3.2.4 Email Services Policy STIG

Policies that govern DoD installations are non-technical directives that must be part of every Exchange security review. Included are items such as performing regular conformance reviews, backups, and role-based assignment separation. Policies contribute to best practices for security in depth and continuity of operations.

Policies review is required for every email domain, regardless of the deployed email services product.

3.3 Email Data Overview

Email data travels on two paths. One is the message transport path, which primarily uses SMTP and moves messages from one domain location (the sending domain) to another (the receiving domain). Process steps for email messages as they traverse the message transport path include domain identification, session encryption and authentication, message sanitization for spam and virus content, and message delivery to identified recipients.

The other path is the “message access” path, which enables users to reach their delivered messages or create new messages. It is typical for sites to offer more than one message access path for users to access messages, as users often travel off-site or require multiple devices that are email enabled.

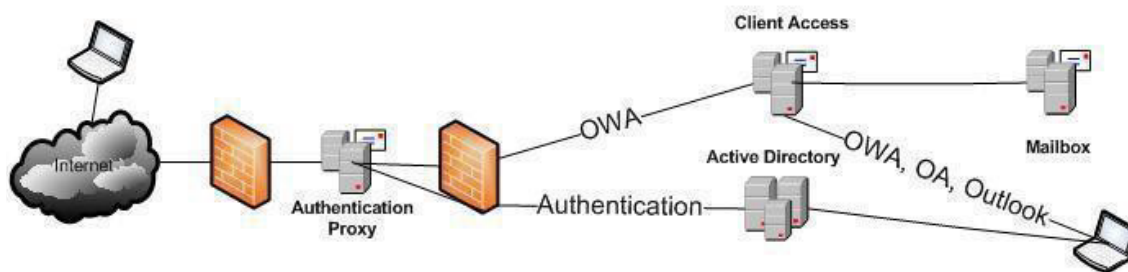
Message access paths include MS Outlook client, Outlook Web App (OWA), Outlook Anywhere, and Active Sync (mobile devices).

Email threats include spam and spoofed content, often inserted at an unsecured point in the message transport path. Inbound email often contains phishing and pharming attacks, forged messages, or embedded malware, or may be signed with a counterfeit certificate, all created to compromise email recipients’ systems or data. Appropriate security measures that prevent unsecured insertion points in the message transport path are essential in preventing most spam. Other measures include processes to evaluate sending domains, message content, or attachment composition. Each of these results can then be used to “score” and possibly filter suspicious messages if they appear to be a potential problem for the recipient.

3.4 Message Access Path

A number of network paths enable end users to access messages on mailbox servers. For local users inside enclave environments, local area networks (LANs) provide the most direct access for desktops, provided they are configured with Outlook and CAC authentication hardware and software. Off-site users may also have access to Virtual Private Network (VPN) connectivity, which enables use of Outlook from off-site locations. For sites offering OWA, off-site users may elect to access email messages using browsers (such as MS Internet Explorer [IE] 8.0) with an Internet connection.

All client requests for message access use HTTP to attach to the Client Access server. The CA server then issues Remote Procedure Calls (RPC) to the user mailboxes. Use of OWA from remote locations, such as the public Internet, must use TLS but authenticate and off-load encryption prior to entering the enclave to enable traffic inspection. The proxy server can then impersonate the requestor for the remainder of the access request.

Figure 3-2: Message Access Path

3.5 Message Transport Path

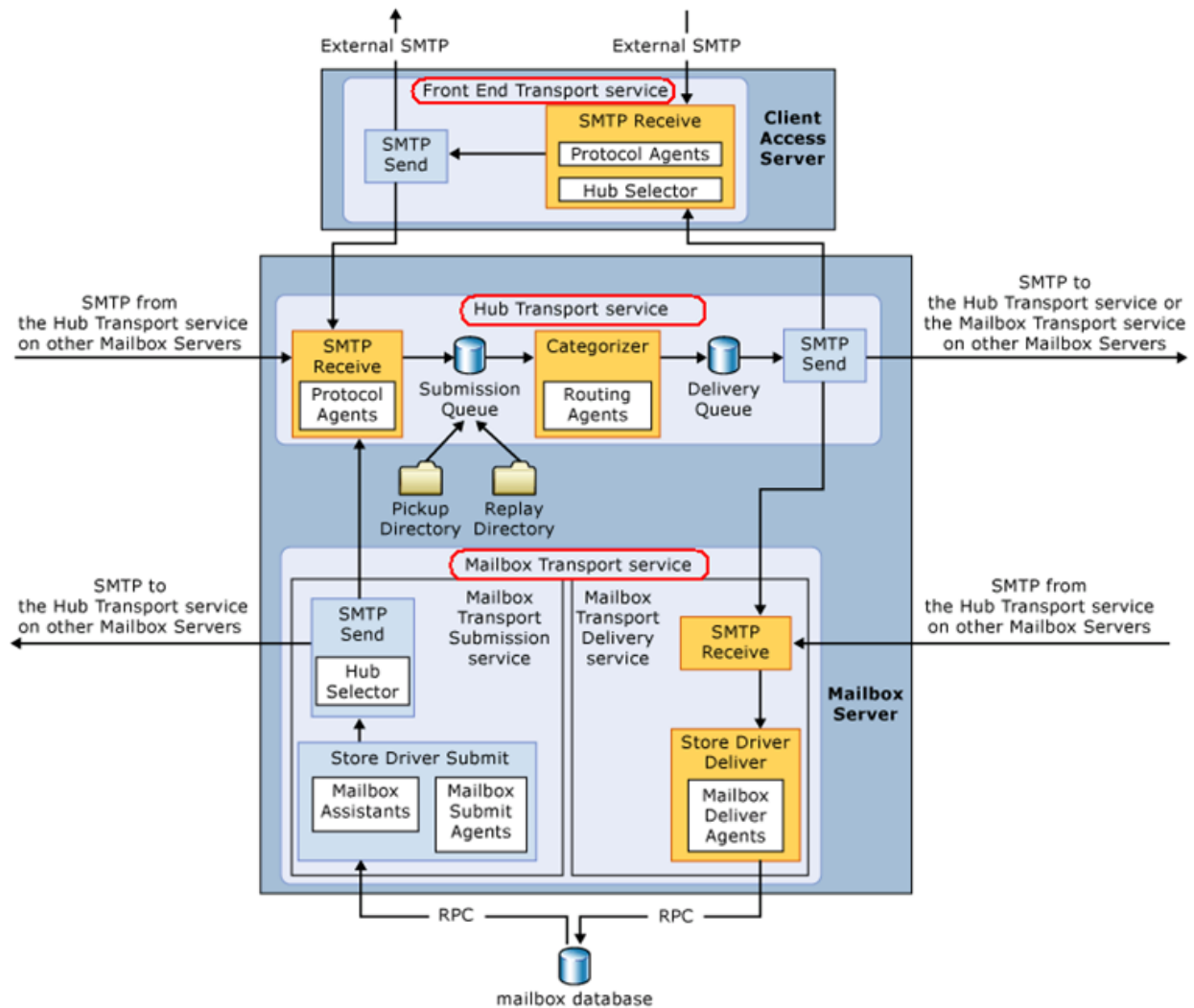
Message transport primarily uses SMTP. SMTP was not created with security in mind; therefore, all security precautions are add-ons that aid with confidentiality and integrity protection while en route to their destinations.

While being transported, messages are relayed from server to server, sometimes crossing unsecured networks, such as the public Internet. In such environments, messages can be trapped, modified, copied, or subject to other mischief during unsecured SMTP message transfer.

It has become a tenet of email message delivery that all message hand-offs be managed using authenticated connections and TLS encryption using server certificates. By eliminating unsecured transport connections, the risk of spam insertion is significantly reduced.

Because email domains must interact with other domains originating across unsecured networks, it is critical that a robust Edge Transport Server role be deployed as the first point of contact for inbound message delivery requests. By using a number of techniques, an Edge server's tasks examine and evaluate attributes of the source domain, the message envelope, and the rate for spam and malware potential. Careful examination of inbound messages helps protect the enclave from Internet-sourced threats. Similarly, outbound message scanning helps protect the domain from reputation damage by ensuring domain-based threats are thwarted before being transported to remote email domains.

Once admitted to the email environment, messages are handed to a Client Access server, whose role is similar to that of a traffic manager. The Client Access server directs messages to users' mailbox servers, where they can be accessed by email-enabled domain users.

Figure 3-3: Message Transport Path

4. REFERENCE DOCUMENTS

The following table enumerates the documents and resources referenced:

Table 4-1: Reference Documentation

Date	Document Description	Source
February 2014	Microsoft Exchange Server 2013	https://technet.microsoft.com/en-us/library/bb124558(v=exchg.150).aspx
Current Version	Windows Server 2008 R2 STIG	http://iase.disa.mil/stigs/os/Pages/index.aspx
Current Version	Windows Server 2012 STIG	http://iase.disa.mil/stigs/os/Pages/index.aspx
April 2013	SP 800-53 Security and Privacy Controls in the Federal Information Systems and Organizations	http://csrc.nist.gov/publications/PubsSPs.html
February 2006	SP 800-18 Guide for Developing Security Plans for Federal Information Systems	http://csrc.nist.gov/publications/PubsSPs.html
February 2007	SP 800-45 Guidelines on Electronic Mail Security	http://csrc.nist.gov/publications/PubsSPs.html
April 2015	Network ports for clients and mail flow in Exchange 2013	https://technet.microsoft.com/en-us/library/bb331973(v=exchg.150).asp

5. CONCEPTS AND TERMINOLOGY CONVENTIONS

5.1 Operational View

Email systems are composed of multiple products and services working together to enable transport and delivery of messages to users. This overview gives background and information specific to MS Exchange email servers. Included also are security review considerations to prepare for periodic assessments.

The associated STIGs provides security policy and configuration requirements for the MS Exchange Server 2013 application. There have been a number of architectural and fundamental changes in Exchange 2013. One change to the Exchange 2013 architecture is server roles. MS Exchange Server 2013 only has three server roles, compared to the five in MS Exchange 2010: Mailbox Server, Client Access Server, and Edge Transport Server, which was introduced with MS Exchange Server 2013 SP1.

An Email Services Policy STIG is also available that governs DoD installations that are non-technical directives and must be part of every Exchange security review.

The MS Exchange Server 2013 STIGs and Email Services Policy STIG can be referenced on the IASE (Information Assurance Support Environment) website at the following URL:
<http://iase.disa.mil/stigs/app-security/app-servers/Pages/index.aspx>.