

**Management Module Firewall Rules for Storage Applications**

**Synopsis:** The purpose of this document is to outline the protocols and port requirement for storage management applications running on the management module for firewall access.

**Authors:** Arpit Roy

**Contributors:**

**Document Version:** 1.0

**Date:** 11/11/2017

**CONFIDENTIAL INFORMATION**

This document contains information proprietary to Thomson Reuters and may not be reproduced, disclosed or used in whole or part without express permission of Thomson Reuters.

© Thomson Reuters 2017

Contents

[1.1 What is a management module? 3](#_Toc498369166)

[1.2 What changes are being made to the firewall rules for management module? 3](#_Toc498369167)

[1.3 Ports that need to be enabled for mgmt module firewall access 3](#_Toc498369168)

[1.3.1 OCUM: Protocol and port requirement 3](#_Toc498369169)

[1.3.2 WFA: Protocol and port requirement 4](#_Toc498369170)

## What is a management module?

A management module is a secure, firewalled environment that hosts the applications necessary for administering our CIS and CPS environments. These applications include DFM/OCUM servers and jump servers.

Benefits of running these applications in their own module:

**Security**: Systems administrators and developers will access their tools in the management module instead of going all the way into the CIS/CPS modules where live data and products are kept.

**Business Recovery**: In the event of a data center outage, all of the critical administrative applications are consolidated in one place instead of being scattered across which helps in quicker recovery.

## What changes are being made to the firewall rules for management module?

Networking team is working to remove the “any any allow” rule on the mgmt module firewalls and replace with rules for given capabilities (project [FAQ](https://thehub.thomsonreuters.com/message/645353)).

Right now, all MGMT module devices (storage owned or otherwise) can access all CPS/CIS filers.

The idea is to a create a standard to not permit storage access between modules (mgmt/corp/ecom/beta/trta  etc).

Suggested solution:

* MGMT assets must only use MGMT filers.
* Filers are for use ‘in-module’ only.

## Ports that need to be enabled for mgmt module firewall access

### OCUM: Protocol and port requirement

|  |  |  |  |
| --- | --- | --- | --- |
| **Protocol** | **Port** | **Description** | **Direction** |
| HTTP | 80 | Used to access the Unified Manager web UI; automatically redirects to the secure port 443 | Both |
| HTTPS | 443 | Used to securely access the Unified Manager web UI or to make API calls; API calls can only be made using HTTPS | Both |
| SSH, SFTP | 22 | Used to access the maintenance console and retrieve support bundles | Both |
| MySQL | 3306 | Used to enable OnCommand Workflow Automation and OnCommand Report access to Unified Manager | Both |
| Microsoft-DS, NetBIOS-ssn, AD LDAP, AD LDAPS | 445, 139, 389, 636 | Microsoft Active Directory LDAP authentication | Outgoing |
| SMTP | 25 | Mail notification | Outgoing |
| SNMPv1 or SNMPv3 | 162/UDP | Used to send alert notification SNMP traps | Outgoing |
| NTP | 123/UDP | Used to synchronize the time on the Unified Manager server with an external NTP time server | Outgoing |

### WFA: Protocol and port requirement

|  |  |  |  |
| --- | --- | --- | --- |
| **Protocol** | **Port** | **Description** | **Direction** |
| HTTP, HTTPS | 80, 443 | Opening WFA GUI and logging in | Incoming |
| HTTP, HTTPS, SSH | 80, 443, 22 | Command execution (ZAPI, PowerCLI) | Outgoing |
| Microsoft-DS, NetBIOS-ssn, AD LDAP, AD LDAPS | 445, 139, 389, 636 | Microsoft Active Directory LDAP authentication | Outgoing |
| SNMP | 161 | Sending SNMP messages on the status of workflows | Outgoing |
| MySQL | 3306 | Caching read-only user | Both |
| SMTP | 25 | Mail notification | Outgoing |
| HTTP, HTTPS, SMTP | 80, 443, 25 | Sending AutoSupport messages | Outgoing |
| Syslog | 514 | Sending logs to a syslog server | Outgoing |
| HTTP, HTTPS | 8088, 8488 | Performance advisor | Both |
| RDP | 3389, 5616 | For remote desktop access | Both |