

**Network Management System Tools**

|  |  |
| --- | --- |
| Number: | IOPS-RUN-0003 |
| Business Unit: | IT Infrastructure Operations |
| Owner: | Matthew Horowitz |
| Email: | Matthew.horowitz@msg.com |
| Written by: | Adrienne.myers@msg.com |
| Go Live Date: | [Publish Date] |

# Foreword

The following Runbook is part of a series of Network Engineering Runbooks. This runbook describes the Network Management System tools utilized by Network Engineering and Network Operations to manage, monitor, and maintain the MSG Enterprise Network.

**Contents**

[Foreword 1](#_Toc28072657)

[1 Purpose and Goals 3](#_Toc28072658)

[1.1 Abstract 3](#_Toc28072659)

[1.2 Audience 3](#_Toc28072660)

[1.3 Scope 3](#_Toc28072661)

[2 Access 3](#_Toc28072662)

[2.1 Secure Shell (SSH) Terminal Emulators 3](#_Toc28072663)

[2.2 RADIUS Server https://10.200.100.38 3](#_Toc28072664)

[3 Accounting and Configuration 3](#_Toc28072665)

[3.1 Cisco Prime – https://10.200.9.120 3](#_Toc28072666)

[3.2 Cisco DNA – https://10.202.9.211 4](#_Toc28072667)

[4 Performance Management 4](#_Toc28072668)

4.1 SolarWinds Network Performance Monitor (NPM) – https://10.202.5.20 4

[4.2 Kiwi Syslog Server – https://10.200.100.232 4](#_Toc28072670)

[4.3 Riverbed 4](#_Toc28072671)

[5 Protocol Analysis 4](#_Toc28072672)

[5.1 Wireshark 4](#_Toc28072673)

[5.2 ProcMon – Process Monitor 5](#_Toc28072674)

[5.3 LanSweeper 5](#_Toc28072675)

[6 DNS, DHCP, IP Address Management (DDI) 5](#_Toc28072676)

[6.1 BlueCat 5](#_Toc28072677)

[7 Wireless Management 6](#_Toc28072678)

[7.1 Cisco Wireless Lan Controller (WLC) 6](#_Toc28072679)

[8 Security 6](#_Toc28072680)

[8.1 Forescout 6](#_Toc28072681)

[8.2 Firewall Management Software 7](#_Toc28072682)

[8.2.1 Panorama 7](#_Toc28072683)

[8.2.2 Cisco Adaptive Security Device Manager (ASDM) 7](#_Toc28072684)

[8.2.3 Firepower 7](#_Toc28072685)

[9 Review and Approval 7](#_Toc28072686)

# Purpose and Goals

## Abstract

This runbook describes the Network Management System tools utilized by the MSG Network Engineering and Network Operations to manage, monitor, and maintain the MSG Enterprise Network.

## Audience

The intention of this document is to be used by MSG Network Engineers, Network Operations personnel, Network Administrators, Systems Administrators, and any employee, contractor, or vendor who have a legitimate business need to utilize MSG network management tools.

## Scope

This document describes and provides access methods for the tools used to manage fault, configuration, accounting, performance, and security of the MSG enterprise network.

# Access

## Secure Shell (SSH) Terminal Emulators

Network management kjpersonnel use secure shell (ssh) terminal emulation to communicate with network devices e.g. routers and switches.

PuTTY and SecureCRT are the two ssh terminal emulators employed most often at MSG. PuTTY is open source. Secure CRT requires a license. See the MSG Network Management Tool GUI Access Workbook to obtain license information.

Download PuTTY - <https://www.putty.org>  
Download SecureCRT - <https://www.vandyke.com/cgi-bin/releases.php?product=securecrt>

Both PuTTY and Secure CRT are available in 32bit and 64bit MS Windows versions. To determine the bit size of your MS Windows PC, go to Start/Control Panel/System and Security/System.

## RADIUS Server [https://10.200.100.38](%20https://10.200.100.38)

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol, operating on port 1812 that provides centralized Authentication, Authorization, and Accounting (AAA) management for network management personnel who connect and use MSG network services. MS Windows credentials are necessary for access to the RADIUS server.

# Accounting and Configuration

## Cisco Prime – <https://10.200.9.120>

Cisco Prime delivers visibility and diagnosis of MSG [Cisco Wireless LAN Controllers](https://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html) and [Cisco Aironet access points](https://www.cisco.com/en/US/products/ps5678/Products_Sub_Category_Home.html). Local credentials are necessary for access to Cisco Prime.

## Cisco DNA – <https://10.202.9.211>

Cisco DNA is the enterprise network management platform for Cisco devices. It is currently only managing devices in the MSG Arena located in 4Penn, New York City. Cisco DNA requires Active Directory credentials to gain access.

# Performance Management

## SolarWinds Network Performance Monitor (NPM) – <https://10.202.5.20> or <https://msgswapp01.thegarden.com/orion>

SolarWinds NPM monitors the performance and availability of MSG enterprise network devices. SolarWinds NPM monitors the performance and availability of MSG enterprise network devices. MS Windows credentials are required for access to SolarWinds NPM.

## Kiwi Syslog Server – <https://10.200.100.232>

The MSG Kiwi syslog server collects, parses, stores, analyzes, and explains syslog messages to network administrators, helping to improve the stability and reliability of the network. Active Directory credentials are necessary for access to Kiwi Syslog server.

## NetScout - ???

## Riverbed

Riverbed software provides a complete digital networking solution to help MSG achieve best-practice standards in business agility, efficiency and innovation. See Table 1. Riverbed requires MS Windows credentials for access. See MSG Network Management Tool GUI Access Sheet in the Network Documentation Teams site for additional access information.

Table - Riverbed Access Information

|  |  |  |
| --- | --- | --- |
| SteelCentral NetProfiler 2270 | SteelCentral NetShark 2170 (AppResponse) | SteelCentral Flow Gateway |
| Hostname: netprofiler | Hostname: appresponse | Hostname: flowgateway |
| https:// 10.200.9.40 | <https://10.200.9.46> | <http://10.200.9.44> |

|  |  |
| --- | --- |
|  |  |

# Protocol Analysis

## Wireshark

Wireshark is a free and open-source network protocol analyzer that enables Network Management personnel to browse the data traffic on MSG’s network interactively.  
Download Wireshark [- https://www.wireshark.org/#download](file:///C:\Users\myersadr\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\DM6LZG06\-%20https:\www.wireshark.org\%23download)

## ProcMon – Process Monitor

Process Monitor is a free tool from Windows Sysinternals, part of the Microsoft TechNet website. The tool monitors and displays in real-time all file system activity on a Microsoft Windows operating system. It is used in system administration, computer forensics, and application debugging. Download – ProcMon [- https://docs.microsoft.com/en-us/sysinternals/downloads/procmon](file:///C:\Users\myersadr\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\DM6LZG06\-%20https:\docs.microsoft.com\en-us\sysinternals\downloads\procmon)

## LanSweeper

Lansweeper is an application that gathers hardware and software information of MSG computers and other devices on MSG’s network for management and compliance and audit purposes. Download Lansweeper - <https://www.lansweeper.com/download/>

# DNS, DHCP, IP Address Management (DDI)

## BlueCat

BlueCat serves as a single source of truth for MSG’s DNS, DHCP, and IP address management. BlueCat manages DDI throughout the company.

Table - Blue Cat Server Access Information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Server name | Network IP Address | Services IPv4 Address | Hostname | Location | Type |
| msgbca-2penn01 | 10.200.100.61 | 10.200.9.101 | msgbca-2penn01.thegarden.com | Manhattan/NY | BC - 45 |
| msgbca-4penn01 | 10.202.5.61 | 10.202.9.101 | msgbca-4penn01.thegarden.com | Manhattan/NY | BC - 45 |
| msgbca-chica01 | 10.63.2.11 | 10.63.3.11 | msgbca-chica01.thegarden.com | Chicago (US CHI) | BC - XMB3 |
| msgbca-losan01 | 10.200.129.5 | 10.200.141.5 | msgbca-losan01.thegarden.com | California (US CA2) | BC - 20 |
| msgbca-sanfran01 | 10.208.8.17 | 10.208.16.17 | msgbca-sanfran01.thegarden.com | San Francisco (AR SFO) | BC - XMB3 |
| msgbca-sanfran02 | 10.208.8.18 | 10.208.16.18 | msgbca-sanfran02.thegarden.com | San Francisco (AR SFO) | BC - XMB3 |
| msgbca-tarry01 | 10.200.207.12 | 10.200.207.45 | msgbca-tarry01.thegarden.com | Tarrytown (US TWZ) | BC - XMB3 |
| msgbca-ventu01 | 10.200.221.36 | 10.200.221.52 | msgbca-ventu01.thegarden.com | Manhattan/New York (US MNH) | BC - XMB3 |
| msgbca-westch01 | 10.201.199.46 | 10.200.199.45 | msgbca-westch01.thegarden.com | Westchester County Apt (US HPN) | BC - XMB3 |

# Wireless Management

## Cisco Wireless Lan Controller (WLC)

A wireless LAN (or WLAN) controller is used in combination with the [Lightweight Access Point Protocol](https://en.wikipedia.org/wiki/Lightweight_Access_Point_Protocol) (LWAPP) to manage light-weight access points in large quantities by the network administrator. The [wireless LAN](https://en.wikipedia.org/wiki/Wireless_LAN) controller is part of the Data Plane within the Cisco Wireless Model. The WLAN controller automatically handles the configuration of wireless [access points](https://en.wikipedia.org/wiki/Wireless_access_point).

Table - Cisco WLAN Controller Access Information

|  |  |
| --- | --- |
| Cisco WLC Location | IP Address |
| Arena WLC | <https://10.202.1.73> |
| Beacon WLC | <https://10.200.75.15> |
| Chicago WLC | <https://10.63.3.15> |
| Forum WLC | <https://10.200.129.51> |
| MSG WLC | <https://10.200.100.24> |
| Pier 1 WLC | <https://10.208.8.14> |
| Practice Facility WLC | <https://192.168.100.10> |
| RCMH WLC | <https://10.129.60.51> |
| Ventures WLC | <https://192.168.5.12> |

# Security

## Forescout

The Forescout platform provides MSG with situational awareness of the extended enterprise and the ability to orchestrate actions to reduce cyber risk.

Table - Forescout Access Information

|  |  |  |
| --- | --- | --- |
| Hostname | IP Address | Location |
| MSGFSM-4Penn01 | <https://10.202.9.155> | Arena |
| MSGFSC-4Penn01 | <https://10.202.9.156> | Arena |
| MSGFSC-4Penn02 | <https://10.202.9.157> | Arena |
| MSGFSC-2Penn01 | <https://10.200.9.156> | 2 Penn |
| MSGFSC-2Penn02 | <https://10.200.9.157> | 2 Penn |

## Firewall Management Software

* + 1. Panorama

Panorama software enables and facilitates configuration management of MSG’s Palo Alto firewalls.

* + 1. Cisco Adaptive Security Device Manager (ASDM)

Cisco Adaptive Security Device Manager (ASDM) lets you manage the Cisco Adaptive Security Appliance (ASA) firewalls and the Cisco AnyConnect Secure Mobility Client through a local, web-based interface.

* + 1. Firepower

Cisco Firepower provides complete and unified management over MSG’s next-generation Cisco firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.

# Review and Approval

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Name | Title | Signature | Date |
| Author | Adrienne D Myers | Technical Writer |  |  |
| Reviewer | Adriano Sverko | Peer Reviewer |  |  |
| Authorizer | Matthew Horowitz | Director |  |  |

|  |  |
| --- | --- |
| Effective Date: |  |
| Review Date: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Revision History | | | |
| Version | **Date** | **Writer** | **Notes** |
| Draft |  | Tech Writer |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Contributors | | | | |
| Dave Massey | Network Operations Engineer | Alan McKenna | IT Manager |
| Brian Quan | Network Operations Engineer | Ramesh Pathak | Network Engineer |
| Isam Abbas | Network Engineer | Adriano Sverko | Technical Writer |
| Ricky Der |  | Sean Whitacre |  |