# Wi-Fi Standard

## Introduction
In an effort to streamline network operations and support and take advantage of available technological interoperability advancements, OMES Information Services utilizes a single Wi-Fi vendor platform for all wireless and authentication requirements.

## Purpose
This document establishes the OMES standard to use a single Wi-Fi platform. This document also establishes the anticipated timeline to transition from the current Wi-Fi vendor platform to the future Wi-Fi vendor platform.

## Standard
The current equipment manufacturer designated for wireless is Juniper and the platform is Juniper MIST. The original equipment manufacturer designated for network access control is Aruba and the platform is Aruba Clearpass.

The transition from Aruba Mobility to Juniper MIST Wi-Fi is in progress. Juniper MIST continues to use Aruba Clearpass for wireless authentication. The transition from Aruba Mobility to Juniper MIST continues with an objective of utilizing Juniper MIST as Aruba access points are phased out in the future.

No device platforms or models by the OEM are exclusively reserved for use only within a specific environment. Platforms and models are individually selected based upon their availability and the identified requirements of the enterprise-wide environment, associated projects or specific agencies.

The primary functions of Aruba Mobility Wireless/Aruba Mobility Systems and Juniper MIST wireless include, but are not limited to the following:

- Outdoor, rural and campus Wi-Fi coverage for all Oklahoma state offices.
- Single point of management for wireless controllers and access points.
- Cluster-based load balancing of wireless access points and client host traffic.
- High level of integration compatibility with Clearpass authentication features.

The primary functions of Aruba Clearpass Secure Network Access Control/Aruba Clearpass NAC include, but are not limited to the following:

- Broad range of authentication compatibility across multiple industry standard protocols.
- High level of integration with Aruba Mobility and Juniper MIST wireless access management.
- 802.1x authentication services for wired and wireless networks.

## Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

## Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

## Revision history

This standard is subject to periodic review to ensure relevancy.

| | |
|---|---|
| **Effective date:** 03/05/2022 | **Review cycle:** Annual |
| **Last revised:** 10/26/2022 | **Last reviewed:** 08/13/2023 |
| **Approved by:** Joe McIntosh, Chief Information Officer | |