The Scottish Government

## Social Security Programme

## Chief Digital Officer Division

# Hosting Build Support

# Statement of Requirements

Version: 1.0

# 1. Document Control

## 1.1. Document Information

| Doc Ref | Classification | Status | Author | Contact |
|---|---|---|---|---|
| | | | | |

## 1.2. Version Control/Approval

| Date | Updated By | Version | Reason for Change |
|---|---|---|---|
| 26/03/2018 | [redacted] | 0.1 | Initial Draft |
| 28/03/2018 | [redacted] | 0.2 | Updated Draft |
| 28/03/2018 | [redacted] | 0.3 | Updated Draft |
| 29/03/2018 | [redacted] | 0.4 | ANNEX A |
| 01/04/2018 | [redacted] | 0.5 | [redacted] updates |
| 01/04/2018 | [redacted] | 0.6 | [redacted] updates |
| 02/04/2018 | [redacted] | 0.7 | [redacted] updates |
| 02/04/2018 | [redacted] | 0.8 | ANNEX A updates: Network and Security detail |
| 02/04/2018 | [redacted] | 0.9 | Annex B and minor changes |
| 03/04/2018 | [redacted] | 0.10 | Minor changes and clarification requests |
| 03/04/2018 | [redacted] | 0.11 | Minor agreed changes |
| 04/04/2018 | [redacted] | 0.12 | Updated AWS Network Architecture Diagram and Description |
| 06/04/2018 | [redacted] | 0.13 | After procurement comments |
| 06/04/2018 | [redacted] | 0.14 | Update to AWS Network Architecture and description |
| 09/04/2018 | [redacted] | 0.15 | Minor changes |
| 09/04/2018 | | 1.0 | |

## 1.3. Distribution

| Name | Role | Purpose |
|---|---|---|
| [redacted] | [redacted] | Approval |
| [redacted] | [redacted] | Approval |
| [redacted] | [redacted] | Approval |
| [redacted] | [redacted] | Approval |
| [redacted] | [redacted] | Review |
| [redacted] | [redacted] | Review |
| [redacted] | [redacted] | Review |

# 2. Contents

# 3. Executive Summary

Amazon Web Services (AWS) will host the Scottish Government's Social Security Directorate (SSD) Low Income Benefits (LIB) platform with a target go-live date of October 2018.

The supplier is expected to design and implement an AWS cloud hosting infrastructure along with mandatory foundation services by July 31st, 2018.

A High Level Design (HLD) of the AWS Architecture and supporting services has been completed and agreed at the SSD Technical Design Authority (TDA) providing detail such as tooling for automated build and testing, supporting infrastructure services, security components and mandatory network integration.

The appointed supplier will be expected to engage with SSD's Hosting Architecture Review Board for approval, as they complete the level 2 designs, produce the detailed design artefacts and deploy all infrastructure and services. Deploying automated infrastructure in the AWS London region for the Pre-production and Production environments.

The automated infrastructure, supporting services and network integration for the Pre-production environment is required by July 31st in order to facilitate a joined up system integration test for the LIB platform.

The appointed supplier will then be expected to deploy the Production environment with supporting services by August 31st 2018, in order to deploy the LIB platform in production and allow further testing such as testing automated route to live, systems, PEN, load, user acceptance and operational testing before go live in October 2018.

The Scottish Government and its associated bodies align with the UK Security Policy Framework as the overarching policy on protective and cyber security.

In line with the 'Secure by Design' principles of the Social Security Digital and Technology Strategy, the appointed supplier will be expected to fully align to the UK National Cyber Security Centre (NCSC) Cloud Security Principles when designing, building and deploying any cloud environment through this engagement and in accordance with the security requirements set out in Annex D of this SoR.

# 4. Background

As a result of the Smith Commission report, defined in the Scotland Act 2016, the following eleven welfare benefits will be devolved to the Scottish Government over the next 4-5 years:

- Benefits for carers, disabled people and those who are ill: Attendance Allowance (AA), **Carer's Allowance (CA),** Disability Living Allowance (DLA), Personal Independence Payment (PIP), Industrial Injuries Disablement Allowance (IIDB) and Severe Disablement Allowance (SDA).
- Benefits which currently comprise the Regulated Social Fund: Cold Weather Payment (CWP), **Funeral Payment (FP), Sure Start Maternity Grant (SSMG)** and Winter Fuel Payment (WFP).
- Discretionary Housing Payments.

These benefits are currently hosted in separate IT systems, administered by the Department of Work and Pensions. The migration of the benefits will be implemented in a series of waves as part of the wider Programme; the first of which being Low-Income Benefits (LIB comprising CA, SSMG and FP), due for delivery from **October 2018**.

The LIB platform is delivered via the Social Program Management (SPM) solution that is being implemented by IBM and tested by the Scottish Government team. The IBM solution development and test environments are for tactical reasons hosted within an IBM AWS account. The creation and deployment of the Pre-Production or a Production environments for the Social Security Directorate (SSD) are not within the scope of the LIB contract.

The SSD Chief Digital Office Division (CDO) is tasked with designing and implementing a hosting facility within its own Amazon Web Services (AWS) cloud infrastructure account. This deployment will initially host the new LIB SPM solution and associated services with the intent of deploying other applications as requirements arise in future years. The LIB SPM solution will integrate with dependant systems such as those hosted in DWP in order to migrate and leverage existing capability.

The CDO objective is to deliver an automated infrastructure hosting facility for the full path to live but as an interim measure the focus and scope is deliberately limited to Pre-production and Production environments initially. The created hosting environments and wider foundation services need to be capable of future extension to support other devolved benefits plus technology components required as part of the CDO enterprise architecture.

# 5. Introduction

The Social Security Directorate's (SSD) Chief Digital Office (CDO) Division owns the design, build and on-going management of the digital infrastructure and associated technical components required in order to deploy a successful service architecture for the Social Security Agency (SSA). A fundamental building block of the infrastructure is the hosting environments upon which the digital solutions will be implemented, tested and operationally provisioned.

The purpose of this document is to set out what is required from a Supplier contracted to assume delegated responsibility for the operational readiness of the Pre-Production and Production environments. These environments are necessary to successfully launch the new Agency's initial LIB benefits with scaling required for future extension to support delivery of further services and technologies. The intent is to make it easy for a Supplier to understand what needs to be achieved, what SSD have already decided, designed or completed and finally make it easy for the Supplier to set out its tender response.

# 6. Requirements

Scottish Ministers, through the Social Security Directorate's (SSD) Chief Digital Office Division (CDO) will award a contract to a single Supplier who can:

- Demonstrate recent experience of completing low level designs for Cloud infrastructure on an enterprise scale.
- Demonstrate both capability and capacity to undertake the requirements set out in this document and subsequent schedules that will be shared under Non-Disclosure Agreements (NDA) using both infrastructure as code and automated infrastructure approaches.
- Contractually commit to the automated creation of the various cloud infrastructure components required by 31 July 2018 within the Scottish Government AWS account.
- Describe, justify and deliver the optimal core on-site team required to meet the SSD requirements.
- Describe and deliver the necessary transient roles that will be required, with associated and estimated durations.

and demonstrate in their response good experience, understanding and intent across the following dimensions of the requirement: 'what', 'how', and 'do so by':

**What**

The Supplier <u>must</u>:

- Deliver AWS hosted, repeatable, **<u>fully automated</u>** provision of secure infrastructure for:
    - <u>Pre-Production</u> &
    - <u>Production environments</u>
- Implement infrastructure, supporting services and network integration for the pre-production environment by **July 31st 2018** in order to perform a joined up system integration test for the LIB platform. The appointed supplier will be expected to deploy the production environment and all supporting services and external network integration by **August 31st 2018**. Both environments must mature at pace to enable full functionality and the successful completion of specified operational readiness tests in time for the **<u>October 2018</u>** go live date. A pragmatic approach may be possible  for the completion of some activities so long as an operationally acceptable service is delivered on time.
- Utilise a range of AWS infrastructure, security and network services  to enable, support, disaster recovery, the securing and management of the overall cloud infrastructure. It is intended to utilise the AWS Platform services if fit for purpose otherwise the service or component identified can be installed on standard AWS Infrastructure utilising Infrastructure-as-a-Service topology or by leveraging solutions on the AWS marketplace.  Note that solutions other that

standard AWS Platform services are required to undergo a product assessment for suitability.

- Enhance and adopt the delivery plan maintaining a principle of credible but acceptable delivery timescales.
- Produce mobilisation plans, including  a full resource profile.
- Deliver a repeatable, automatically provisioned delivery platform. A platform enabling DevOps tools and processes that support continuous integration with automated running of tests and deployment of  functionality from Development through the 2 new environments.
- Review and adopt the High Level Design (HLD) as agreed at the SSD Technical Design Authority. Seeking change through TDA governance if required.
- Complete the set of level 2 designs and produce the level 3 detailed design artefacts and operational manuals (level 4) - (see annex B for level explanation).
- Defining the Suppliers Operational Readiness Tests for the environments, perform tests,  sharing documented results with SSD and taking corrective action. Working constructively with SSD/partners/stakeholders in their operational testing (providing additional Skills/Capacity if required) to realise a stable, performant, operational service for the Agency's first benefit mechanism.

**How**

The Supplier will

- Ensure that the provision of any and all environments, components and services are delivered in alignment with the UK NCSC Cloud Security Principles, evidenced via a formal report to the Chief Digital Officer at least 14 days before go-live.
- Data processed during this engagement will be handled in line with requirements of the Government Security Classification policy, specifically the requirement for OFFICIAL-SENSITIVE.
- Have 'Infrastructure as Code' and 'Automated Infrastructure' techniques central to the delivery, creating the capability to automate and replicate for the efficient delivery of non-production environments from the delivered instances.
- Deliver DevOps tools and processes to support the migration from the IBM Test and Development environments through to the new Pre-production and Production environments..
- Deploy all infrastructure and services into the SSD AWS account in the AWS London region.
- Co-locate and commit to working effectively with SSD staff throughout the lifetime of the contract, including integrating the existing SSD Hosting team (see annex C) and CDO. Working also with various other key partners such as iTECS, SWAN Capita, IBM and other parts of the Social Security Programme who are developing common components and services for the agency. BPSS clearance will be required for all participating resources (see Annex D – 10 for more detail).

- Assist SSD and nominated third parties for support, deployment and changes on the hosted environments.
- Deliver necessary hands on and documentation knowledge transfer material and sessions for the in-house support team.

**Do So By**

The Supplier must:

- Leverage previous relevant experience of providing such services in an AWS environment using both ‘infrastructure as code’ and ‘automated infrastructure’ approaches. For the avoidance of doubt we do not want anything hand configured within AWS, all parameters and configuration is to be driven by code.
- Assist with the implementation of processes to prevent environment drift via manual changes that are not within code.
- Have the capacity and capability to mobilise the skilled resource and capabilities to meet the defined timescales, in particular the 31 July 2018 date.
- Have a priority focus on pace, enabling delivery within the timescales described in this document.
- Work within a Prince2 Lite project management methodology for overall delivery.
- Use Agile methods to deliver the actual build of the required live service.
- Accept delegated responsibility for delivery while aligning with SSD Governance e.g. TDA and Hosting Architecture Review Board for permission so as to ensure fit for purpose, “secure by design” deliverables and appropriate financial outlay.
- Ensure implementation and delivery costs demonstrably provide value for money.
- Surrender all IPR (including all code, designs, documentation) associated with this engagement to the Scottish Government.
- Work with SSD to utilise the Amazon Market Place where effective to do so.
- Work with SSD to incorporate where relevant and practical Scottish and Central Government IT guidance.
- Provide expert level knowledge and guidance to SSD in applicable subject areas.
- Work with SSD to adhere to the relevant SD/CDO policies and standards.
- Handover responsibility for support and continued infrastructure development (with appropriate design and configuration documentation) to SSD nominated support staff.

## 7. Additional Optional Requirements

The Supplier is required to provide detail for the delivery of additional options that the CDO may choose to have the Supplier deliver. The CDO requires the Supplier to clearly set out these costs and resources separately, from each other and from the main deliverables. The options are:

A. Development, test and training environments: Following creation of Pre-production and Production environments a Development environment will be required. A means to quickly create replica production environments to use as, for example, test and training environments will be required by **28th September 2018**.

B. Operational Support: Support may be required from the Supplier for the deployed infrastructure and associated services. This will be for an initial 3 months period (to be reviewed and potentially extended to 6 months) starting on **31st July 2018** when the first environment is required to be functional. The supplier must also evidence in their response the capability to provide this service and clearly indicate where the support resources will be located. For the avoidance of doubt we will require UK based personnel due to the sensitivity of some of the data being managed.

## AWS Architecture

The supplier will design and build an AWS cloud infrastructure capable of hosting multiple enterprise applications such as LIB. The sections that follow are intended to provide adequate detail to  design and deploy this AWS cloud architecture.

## High Level AWS Architecture

The Platform architecture adopts an approach that delivers a hosting environment to provide isolation and segregation with on-demand infrastructure capabilities.

The AWS infrastructure will be constructed within the UK AWS region with Production, Non-Production, Security and Shared Services isolated in separate  accounts. The AWS 'Organisations' feature will centrally manage payment for resources consumed in the environments as well as providing account policies as outline in Figure 1 – AWS Architecture Overview

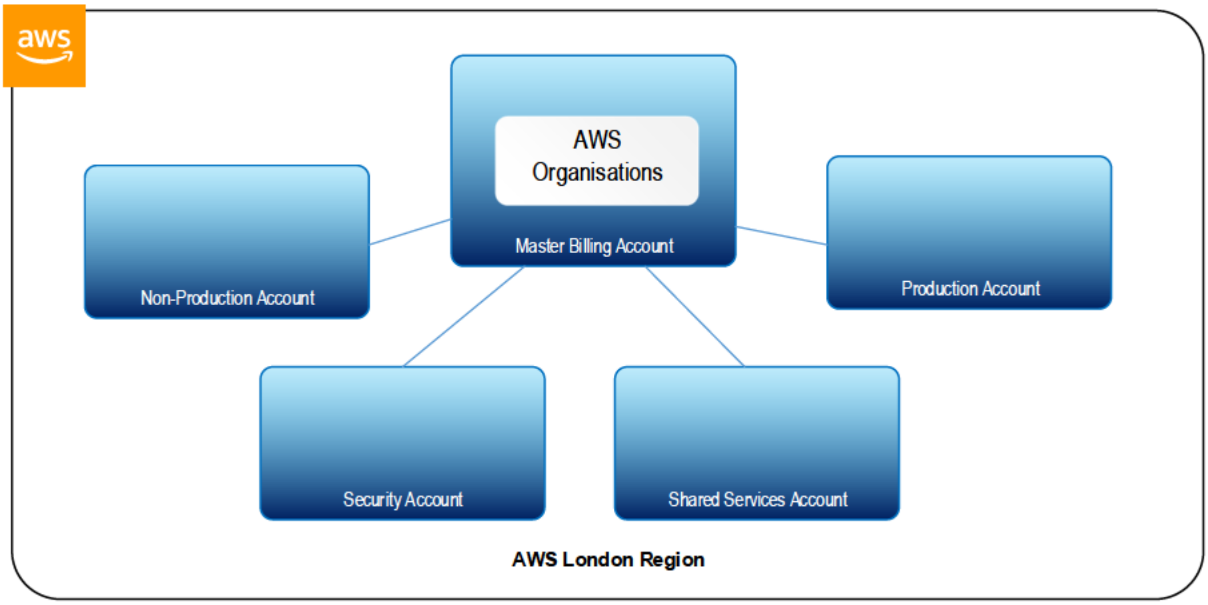


*Figure 2 - AWS Architecture Overview*

The development and test environments are segregated from production services and can capitalise on the three AWS UK availability zones, if appropriate for use, as depicted in Figure 2 –

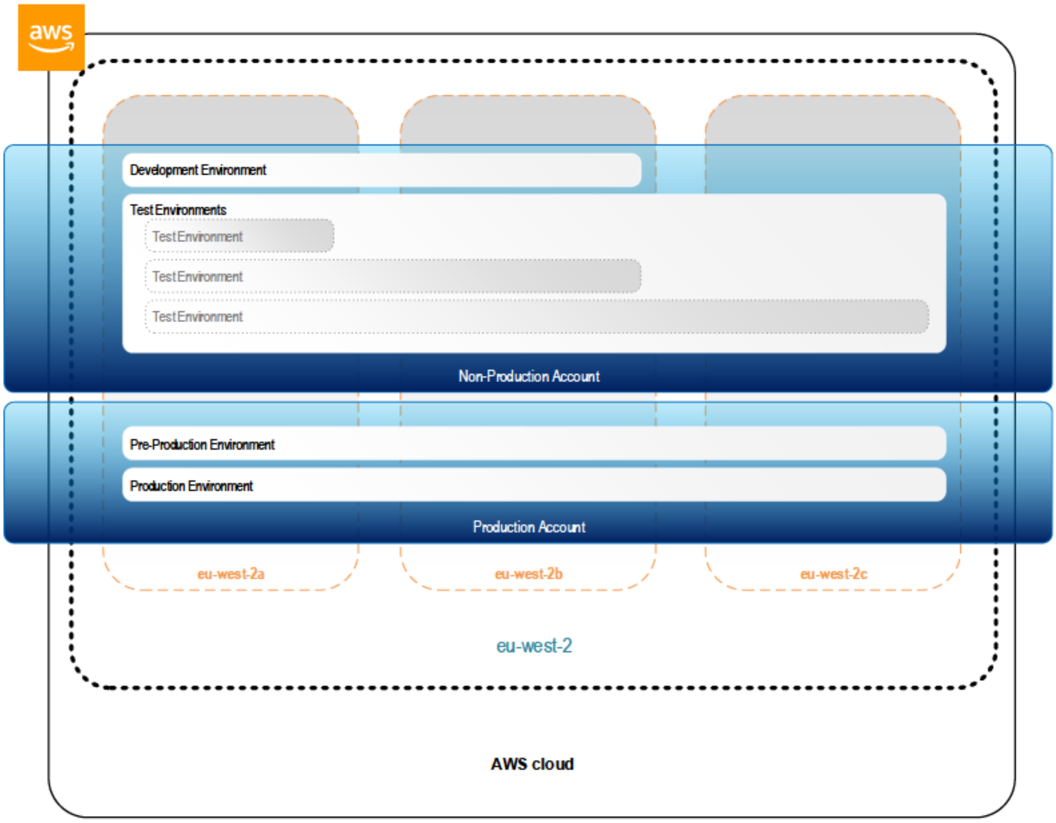


*Figure 2 – Production and Non-Production Architecture*

A high level overview of the AWS Network Architecture is outlined in Figure 3 and described as follows:

- [redacted]

[redacted]

*Figure 3 – AWS Network Architecture*

The AWS architecture will adhere to the following principles:

- All components and services deployed in the hosting environment must be delivered using ‘infrastructure as code’ and ‘automated infrastructure’ with no manual configurations.
- AWS Organisations will be utilised to centrally manage billing and AWS account policies
- All billable AWS resources will be tagged to feed into the AWS Billing and Cost Management reports
- AWS Accounts will be deployed to segregate, isolate, control and secure environments
- Separate VPCs deployed within the Production or Non-Production accounts will isolate the business application stacks from management related services
- The management VPC will host management services that cannot be shared across production and non-production environments such as Active Directory and DNS
- The Shared Services account will host management services that can be shared between environments such as DevOps orchestration tools, Anti-Virus and Vulnerability Scanning
- [redacted]
- The infrastructure and services must be provisioned in an automated and controlled Route to Live deployment with each stage of the lifecycle centrally orchestrated  and secured.
- The AWS Architecture must adhere to Amazon’s best practice architecture principles including but not limited to AWS Accounts and Security, Accounts for Billing and Tagging Strategies.

## AWS Foundation Services

The AWS cloud environment requires a range of infrastructure, security and network services to enable, support, secure and manage the overall cloud infrastructure. It is intended to utilise the AWS Platform services whenever appropriate; however, alternative solutions may be considered should the platform service be unsuitable. Note that solutions other that standard AWS Platform services will require a product selection assessment for suitability.

The following table defines the capabilities that are required by the SSD Hosting Platform.

| Aspect | Description |
|---|---|
| **Active Directory** | An Active Directory Service is required within the AWS cloud environment to centrally manage credentials for engineers and service accounts for *nix and windows platforms. Active Directory will control access to all instances, applications and services deployed in the AWS environment. |
| **DNS** | DNS is required to resolve all hosts and services deployed in the AWS cloud infrastructure. The DNS service should also allow on premise users and services to resolve hosts and services deployed in AWS. |
| **DHCP** | DHCP will be used to provide IP address allocation to instances deployed in AWS VPCs including scope options such as DNS and NTP |
| **Time Services** | A centralised time service is required to ensure time is synchronised across all instances and services deployed |
| **System Monitoring / Alerting** | A system and security monitoring and alerting service is required to provide early warning of service issues.<br>Integration with NCSC Active Cyber Defence (ACD) service – IP/DNS/web checks and phishing service. |
| **Application Monitoring/Alerting** | Basic application monitoring and alerting service is required to provide early warning of service issues |
| **Backup** | Cloud based backup solution required utilising AWS platform. Backup within UK / Application destinations only (GDPR). |
| **Archive** | Design and implement suitable archive solution utilising AWS platform |
| **System Patching** | A solution required to patch all IAAS and marketplace deployments. The solution must allow critical patches to be deployed in short notice in a coordinated and controlled |

| Aspect | Description |
|---|---|
| | manner. The patching solution must integrate with the build of the AMI Gold creation pipeline. |
| **Application Patching** | IBM supply updates to  for LIB platform. Application patching process required to deploy application updates into AMI Gold image creation pipeline. |
| **Bastion Hosts** | [redacted] |
| **Remote Administration** | A remote administration service is required to allow SSD staff to administer services deployed in AWS such as, but not limited to, Active Directory, DNS, Backup, Security Scanning, etc. Solution to be identified, agreed and implemented. |
| **Third Party Access** | Remote access solution required to allow third parties to deploy and managed development and test of code and services. Each third party should be isolated  with access and permissions granted only to restricted areas. Note that IBM must be able to connect to preproduction in order to provide the scripts and artefacts from their AWS account so they can deploy the LIB platform and supporting components. |
| **Centralised Logging** | A centralised logging service is required for system, application, security and AWS service logs. Service must provide reporting functionality. |
| **Internet Proxy** | Proxy service required to provide internet egress service with whitelist and blacklist capability for AWS instances and services |
| **Reverse Proxy** | Reverse proxy capability to control access to internal infrastructure services  such as remote admin facility, third party access, single sign on or DNS integration. |
| **Load Balancing and Auto Scaling** | Load balancing and auto scaling solution required to allow applications and services to be deployed in a highly available architecture and dynamically scaled based on service demand. |
| **Gold AMI Pipeline** | Solution required to create and manage AMI builds containing OS hardening, system\security patches, core applications and components. The service must be fully |

| Aspect | Description |
|---|---|
| | automated with the ability to add, change or update the images as required. This solution must be able to deploy new images through route to live in a controlled and coordinated manner. All images must be hardened to level specified by SSD Security. |
| **Job Scheduling** | The AWS Batch scheduler evaluates when, where, and how to run jobs that have been submitted to a job queue. Jobs run in approximately the order in which they are submitted as long as all dependencies on other jobs have been met |

## AWS Network Architecture

This section outlines the networking and connectivity elements of  the infrastructure architecture to support the SSD Hosted Platform and phase 1 applications.

SSD staff will be located in two new offices located in Glasgow and Dundee. Temporary locations are currently in use to support development and business activities while the permanent locations are being procured and fitted out.  The temporary locations are existing Scottish Government buildings :

- **Atlantic Quay,** Glasgow G2 8LU
- **Victoria Quay,** Edinburgh EH6 6QQ

All networking infrastructure in and between all Scottish government offices are owned and managed by the Scottish Governments iTECS: Data Centre and Network team.

The connectivity use cases for the SSD hosted infrastructure and first application are:

- Public Users: the "citizens" that access the applications via the internet. Public users will access all applications as a web service via a public URL

Max peak concurrent per hour will be 50% of daily (~150 per hour)

| Benefit | 2018/19 | | 2019/20 | |
|---|---|---|---|---|
| | Total Application Volumes | Average Volume | Total Application Volumes | Average Volume |
| LIB | 9400 | 361/week, 72/Day | 73067 | 1964/week, 393/day |

- Business Users: the administrative and support staff that will access the application. These will be  from SCOTS devices on the SCOTS network and browser access only. This will be a separate admin  type login. Single Sign

On will be provided using federated access to the SCOTS LDAP DEVOPS and SCOTS Support Staff. There are <2000 total SSD Business use population estimated for the first 3 years.

- DevOps and support staff: comprise various technical and support roles that will be responsible for developing, deploying, managing and configuring the hosting platform and associated services and application. All access will be route to a “bastion” or “jump” node in the internal DMZ and not directly to the managed resource or devices. The number of required support staff is not known.
- [redacted]

Network access will be from the following devices (varies by role).

- [redacted]
- [redacted] [redacted]

The SSD strategic choice for network connectivity to AWS from SCOTS sites and for all internal user is [redacted] provided by a partner network carrier. Two main partner options have been identified

- [redacted] to AWS utilising existing [redacted] and available 1 Gb internet connection. The lead time for the initial connection is approximately 12 weeks. [redacted] hat can be associated with a single AWS Virtual Interface (VIF)
- [redacted] utilise existing [redacted] in the primary and secondary Scottish Government data centres (Saughton and Caird). Capacity and lead time for this has need yet been confirmed.

It is likely that [redacted] will be the selected network option therefore a dispensation has been created to order these connections ahead of an agreed network design. The four 100 Mb [redacted] hosted connections will be configured as follows:

- Two of the hosted connections will be associated with the Non-Production Transit VPC to isolate management from business application traffic
- Two of the hosted connections will be associated with the Production Transit VPC to isolate management from business application traffic

A Transit VPC topology will be deployed to manage all network routing as outline in Figure 3 and summarised as follows:

- All Production and Non-Production traffic will be routed through separate Transit VPCs
- The Transit VPC will manage the routing of all Internet and Scottish Government network traffic as well as the routing between the Management, Business Applications and Shared Services VPCs
- All Internet traffic will flow through the Internet DMZ zones
- Scottish Government management and business application network traffic will be segregated and routed through the Scottish Government DMZ zones

It is recognised and provisionally agreed with SSD security that given the timescales a secure short term solution utilising a VPN client and VPN Gateway can be used. This will allow connectivity from the DevOps devices to the AWS VPC for build and configuration tasks. These connections will utilise existing SCOTS network infrastructure.

The network design must also take into account any security requirements around perimeter controls and  the implementation of a DMZ (or similar) topology. This is likely to include, but not limited to, typical capabilities such as Network Firewall, WAF, DDOS. Proxy, Reverse Proxy, IDS and security scanning services.

## AWS Security Architecture

In addition to aligning with the NCSC Cloud Security Principles, the AWS security architecture must align with the principles of the AWS Cloud Adoption Framework (CAF). The high level aims are:

- Deploy security infrastructure in alignment to the Security Perspectives of the AWS Cloud Adoption Framework
- Leverage AWS native security capabilities whenever possible and applicable
- Select AWS marketplace or other vendor solutions where AWS native services do not offer a security control.
- Select security controls which fit the current and future SSD Operating Support Model

Under the AWS CAF, there are four security perspectives to be addressed:

1. *Directive* controls establish the governance, risk, and compliance models the environment will operate within
2. *Preventive* controls protect your workloads and mitigate threats and vulnerabilities.
3. *Detective* controls provide full visibility and transparency over the operation of your deployments in AWS.
4. *Responsive* controls drive remediation of potential deviations from your security baselines.

The security capabilities the supplier must design and implement are defined in the table below.

| Aspect | Description |
|---|---|
| **Account Management** | Establish an appropriate Governance model of AWS accounts across the organisation. Creation of procedures to manage AWS accounts in a consistent manner, ensuring control settings are appropriate and that clear ownership is established. |
| **Control Framework** | Ensure AWS service usage aligns to compliance requirements and designed security controls. |
| **Control Ownership** | Definition of a support operating model and RACI for security platform management, event monitoring and response. To ensure security (technical and process) debt and control gaps are not introduced during the design and implementation of the AWS infrastructure. |
| **Least Privilege Access** | Privileged management and application user access controlled via integration with a centralised directory service with single sign-on. Design and build the AWS infrastructure based on the principles of least privilege and strong authentication. Implement protocols to protect access to sensitive credential and key material associated with every AWS account. |
| **Change and Asset Management** | Develop an organisational tagging standard for all deployed AWS resources, e.g. EC2 instances, load balancers, databases, volumes, encryption keys, etc. Leveraging the meta-data supplied by resource tagging enables automation of the deployment and maintenance of security controls including patch management, encryption key management, endpoint AV, etc. |
| **Security Patterns** | Creation of AWS security implementation patterns aligning to SSD Information Security Policies and control frameworks. Establish security designs, standards and guardrails to be referenced by DevOps engineers, Security Engineers, Security Operations. |
| **Identity and Access** | Create access permissions based on organisation role. Ensure access rights are defined based on separation of duties principles. Define roles including AWS Admins, DevOps Engineers, Security Engineers, Security Auditors , etc. Integrate the use of AWS into the AWS hosted environment, as well as into the sources of authentication |

| | |
|---|---|
| | and authorization. Create fine-grained policies and roles associated with appropriate users and groups. |
| **Infrastructure Protection** | • Design and deploy network perimeter firewalls conforming to a transit VPC model.<br>• Provision Web Application firewalls and Application DDOS to protect application workloads with Internet-facing services conforming to a transit VPC model. The solution should capable of policy-based web application security that blocks against OWASP top 10 threats and zero-days attacks. Both AWS hosted and UK-based Software-as-a-Service (SaaS) solutions will be considered.<br>• Provision Network DDOS, , and forward/reverse proxy infrastructure to protect application workloads with Internet-facing services conforming to a transit VPC model.<br>• Provision capabilities to harden and patch EC2 hosted workloads in adherence to security and industry best practices. Continuous automated reporting should be a core function.<br>• Design and implement an AWS hosted Anti-malware/Anti-virus capability covering RedHat and Windows EC2 hosts. Both AWS hosted and UK-based Software-as-a-Service (SaaS) solutions will be considered.<br>• Deploy host-based IPS on EC2 hosted workloads. |
| **Data Protection** | • Encryption Key Management 1: Lifecycle management of keys used to encrypt AWS native services including S3 buckets, RDS databases, EBS volumes, etc.<br>• Encryption Key Management 2: A UK-based tamperproof and secure key management function to support cryptographic operations required for the encryption of DB2 databases (DB2 Transparent Data Encryption), and Active Directory Certificate Services.<br>• Encryption Key Management 3: An AWS hosted secure key management function to provide storage and distribution of SFTP and SSH keys.<br>• Secrets Management: Provision of an encrypted secure repository where DevOps Engineers, IT development, application and security teams can dynamically generate and store secret material, (e.g. |

| | |
|---|---|
| | tokens, passwords, database authentication strings, API access keys, etc.) via an unified API.<br>• Certificate Services 1: Lifecycle management of SSL/TLS Certificates used to secure connections presented by Elastic Load balancers to internally-facing services.<br>• Certificate Services 2: Lifecycle management of SSL/TLS Certificates used to secure connections presented by externally-facing Web Application Firewalls, API Gateways and Elastic Load Balancers. |
| **Logging and Monitoring** | Collection of AWS API, EC2 hosted Operating Systems and Applications security logs to be consumed by the Scottish Government Security Operations Centre. |
| **Security Testing** | Vulnerability and compliance scanning of EC2 hosted operating systems and databases providing a clear view of the security health of the estate. Testing the AWS environment to ensure defined security standards are met. Identification of security vulnerabilities and deviations from best practices. Provision of automated security compliance scanning. Alignment to CIS benchmarks and CVE. |
| **Change Detection** | Implement measures to determine if deployed security controls drift from the implemented security baselines. Detection and prevention of unauthorised changes which weaken the security posture of services hosted within AWS, e.g. enabling open access on S3 buckets, building disk volumes without encryption, changing security groups (i.e. firewall rules) with overly permissive access, disabling audit logs, etc. |
| **Segregated Security Logs** | Security logs, CloudTrail, VPC Flow Logs etc. to be saved to a secure, segregated location. |
| **SOC** | Integration with Scottish Government and SSD SOC Capabilities |

## Deployment Approach

The SSD Hosting platform is to prioritise the adoption of Platform as a Service (PaaS) delivery options whenever appropriate so as to benefit from Economies of Scale, Time to Market and Tried and Tested service scalability and security. Should a PaaS service be considered to be unsuitable, alternative solutions delivered through Infrastructure as a Service (IaaS) may be considered.

SSD will implement technologies and processes that define a software development, testing and delivery pipeline upon the SSD Hosting Platform as previous defined.

The approach adopted in the development and operation of the SSD Hosting platform must enable to the following objectives:

- Enable the automation of application testing, assurance and deployment processes, to ensure the highest level of confidence in service quality can be attained and maintained
- Enable a low mean time between development and deployment
- Enable an on-demand, elastically scalable service

The DevOps approach being adopted by SSD is to focus efforts on rapid IT service delivery through the adoption of agile, lean practices in the context of a system-oriented approach and seeks to improve collaboration between operations and development teams. The DevOps implementation for SSD is to utilise technology — especially automation tools to leverage programmable and dynamic cloud infrastructure to achieve SSD Hosting Platform objectives.

The SSD software development team utilise automated build systems that comprise of version control systems, orchestration, standardised build processes, static code analysis and delivery pipelines. The SSD hosting platform must enable the application development, testing and release lifecycles and the adoption of two practices – Continuous Integration (CI), Continuous Delivery (CD). The aforementioned SSD hosting platform objectives are to be achieved through the utilisation of Infrastructure as Code.

CI will be an automated practice where code changes trigger the execution of a suite of tests upon standardised build and test environments. Each check-in is verified by the automated build and test execution, allowing teams to detect problems early.

Adopting a CD approach must result in always being in a position of having software that is in a releasable state, however the software may not necessarily be feature-complete. Most importantly, not every release will be deployed to production.

To enable the desired CI / CD practices adopted by SSD application development, testing and release lifecycles, infrastructure operations are to define all infrastructure (Servers, Network, Supporting Services) in code and establish secure management of configurations and the reliable automation of environment and application provisioning. More than simply writing scripts, the approach adopted must follow tried, tested and proven practices that work in harmony with application development. For example: version control, testing, small deployments, use of design patterns etc.

**Selected Tools**

Development Platform

- [redacted]

Hosting Platform – DevOps

- [redacted]

**Example Development Release Flow**

1. Business Analyst obtains and documents requirements from Product Owner in the form of use cases and stories
2. Developers implement requirements through iterative periods of focussed effort called sprints.  Distinct units of code functionality are produced with accompanying tests, referred to as unit tests.  Development teams are responsible for ensuring that all tests pass before committing changes to the shared code repository;
3. Upon source code commit, the build environment will automatically trigger a build of the product suite.
   3.1. Code is compiled
   3.2. Static Code Quality Analysis Checks are executed;
4. Upon a successful build (All compilation, tests and quality checks passed), the compiled output (Artefact) of the build is stored in an artefact repository;
5. Upon the availability of new artefacts, an automated orchestration process is invoked which oversees the systematic testing of releases through the preparation and destruction of on-demand development, test environments infrastructure:
   5.1. Dev Testing
      5.1.1. Environment is built;
      5.1.2. Unit tests are executed;
      5.1.3. SIT are executed;
      5.1.4. Performance and Operational tests are executed;
      5.1.5. Security tests are executed;
      5.1.6. Environment is destroyed;
   5.2. UAT Testing
      5.2.1. UAT Environment is built;
      5.2.2. UAT tests are executed;

5.2.3. UAT Environment is destroyed;

6. A distributable artefact, with reliability proven through all quality gates, is published to the production artefact repository, ready for deployment upon the production environment on-request of the release manager.

## Route to Live

All development and test cycles will be performed in the non-production account utilising the deployment approach described above with each environment securely segregated and isolated.

## LIB Platform Application and Services

IBM are currently developing the SSD LIB platform within an IBM owned and managed AWS cloud infrastructure. This platform will be deployed into the SSD AWS hosted environment for end to end systems integration test on July 31st, 2018

[redacted]

IBM require access to SSD's AWS environment in order to perform an automated build of the LIB platform and supporting components followed by a  series of tests, before the planned go live date of October 31st, 2018.

The supplier must provide network connectivity between the Scottish Government AWS account and the IBM Dev/Test account to allow IBM to connect securely to the SSD AWS preproduction and production environments. IBM will provide (and execute) scripts and artefacts, within IBM's AWS Development account (located in GitLab and Artifactory repositories) in order to build GitLab, Artifactory, and orchestration services within the AWS SSD management zones. These services will then allow IBM to automate the deployment of the LIB platform within SSD.

IBM also require access to the AWS portal and APIs with sufficient IAM permissions to deploy components into both SSD nonproduction and production environments such as, but not limited to, EC2 instances, volumes and security groups. Exact permissions will be clarified.

## Non-Functional Requirements

The hosting platform and corresponding services deployed must be capable of supporting the NFRs outlined below. These NFRs apply to applications and services deployed within the cloud infrastructure such as LIB therefore the supporting infrastructure, network and security services must also adhere to these requirements.

| Non Functional Requirement |
|---|
| The LIB Production Core System shall support up to 2,000 registered users with up to 400 concurrent users |
| The services deployed must allow business applications and services to be resilient, high availability, providing application operational availability of 99.99% and application reliability of 99.0% during the System online-day. During this time all System user dialogues and message-based interfaces shall be available and fully functioning. |
| All supporting services must be resilient and highly available within the production environment ensuring service continuity in the event of component failure or loss of an availability zone. |
| Recovery time objective of less than 4 hours. |
| Recovery point objective of last committed transaction |
| All Systems shall comply fully with the SSD's Technology policy and standards/objectives for:<br>Data replication<br>Data integrity/error messages<br>User Access<br>System Administration |
| The platform must be designed to support scheduled batch processing and the ability to automatically exchange these files with third parties such as DWP |
| Under normal operation conditions the production system used to send files generated by batch should process within the following timeframe:<br>95% of these messages shall complete in less than 2 seconds<br>99% of these messages shall complete in less than 3 seconds |
| The supporting services must be capable of allowing AEM to be operational near 24*7 |
| The supporting services must allow SPM to be available for on-line use from Monday to Friday 07:00 – 19:30, and Saturday 07:00 - 17:00 (excluding only Non-Working Days). |
| The SPM System Production Environment is a high availability system, providing application operational availability of 99.999% and application reliability of 99.0% during the SPM System online-day. During this time all SPM System user dialogues and message-based interfaces must be available and fully functioning.<br>The supporting services deployed must provide this capability. |
| Single points of failure need to be minimized in both the application and underlying infrastructure. |
| All single points of failure need to be highlighted with recovery procedures agreed and implemented |
| Back up of the end-to-end solution must be automated and require no end-user intervention. |

| |
|---|
| The backup approach must allow the restoration of the System to a known point and consistent state. |
| All production services  must be able to scale resources, both automatically or manually, and to meet service demand. |
| Systems must be capable of providing performance and service data at appropriate frequencies to support service and performance levels and reporting. |

# ANNEX B

The SSD CDO Hosting Platform Team have established a standardised definition for the detail level of each document artefact, with the purpose of describing the level of detail and complexity to be expected from the documentation, and the level of technical understanding required by the intended reader. These levels are defined as:

| **Definition** | **Intended Audience** | **Responsible to deliver** |
|---|---|---|
| **Level 1 –** High Level Design | General | SSD |
| **Level 2 –** Detailed Implementation Definition and Design | Technical Executive | Supplier |
| **Level 3 –** Implementation / Automated Deployment | Architect/Engineer | Supplier |
| **Level 4 –** Run Book / Operations Manuals | Engineer | Supplier |
| | | |

# ANNEX C

The SSD CDO Hosting Platform Team will:

- perform the assurance role for SSD across the whole delivery. This will take the form of governance at TDA and Architecture Review Forum but also general review of the required design deliverables and the implementation itself.

- facilitate progress where internal Scottish Government factors are impacting delivery.

- will contribute hands on management and technical output / insight where the capacity of the team allows.

TDA

| | | |
|---|---|---|
| [redacted] | [redacted] / Chair | Owner |
| [redacted] | [redacted] | Assuror |
| [redacted] | [redacted] | Assuror |
| [redacted] | [redacted] | Assuror |
| [redacted] | [redacted] | Assuror |
| [redacted] | [redacted] | Assuror |
| [redacted] | [redacted] | Assuror |
| [redacted] | [redacted] | Assuror |

Hosting Architecture Review Board

[redacted] (Solution Architect and Chair)

[redacted] (Technical Lead)

[redacted] (Platform Owner and Secretary)

[redacted] (Security Architect)

Hosting Platform Team

- [redacted] Platform Owner / Project Manager)
- [redacted] (Technical Lead)
- [redacted] (DevOps Architect / Lead)
- [redacted] (Infrastructure & Network)
- [redacted] (Security Architect)
- Scrum Master (TBC)
- Network Architect (TBC)

# ANNEX D

## Security Requirements

| | |
|---|---|
| "Data" | ‘Data’ refers to<br>(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:<br>(i) supplied to the Service Provider by or on behalf of the Scottish Government; or<br>(ii) which the Service Provider is required to generate, process, store or transmit pursuant to this Contract; or<br>(b) any Personal Data for which the Scottish Government is the Data Controller; |
| “Good Industry Standard” | means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “IT Security Health Check” | means an assessment to identify vulnerabilities in IT systems and networks which may compromise the confidentiality, integrity or availability of information held on that IT system. |
| “NCSC” | is the UK government’s National Cyber Security Centre and is the National Technical Authority for Information Assurance. The website is http://www.ncsc.gov.uk/ |

1. The Service Provider will be expected to have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements) or equivalent. The ISO/IEC 27001 certification (or equivalent) must have a scope relevant to the services supplied to, or on behalf of, the Scottish Government and the statement of applicability must be acceptable to the Scottish Government, including the application of an appropriate selection of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

•

2. The Service Provider will adopt the UK Government Security Classification Policy in respect of any Scottish Government data being handled in the course of providing this service, and will handle this data in accordance with its security classification. In the event where the Service Provider has an existing Protective Marking Scheme then the Service Provider may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Scottish Government data.

•

3. Scottish Government data being handled in the course of providing this service must be segregated from other data on the Service Provider's own IT equipment to protect the Scottish Government data and enable it to be securely deleted when required. In the event that it is not possible to segregate the Scottish Government data then the Service Provider is required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 9.

•

4. The Service Provider, on their own ICT systems and endpoints will have in place and maintain technical safeguards to protect Scottish Government data, including but not limited to: Good Industry Standard anti-virus and firewalls; up-to-date patches for operating system, network device, and application software. Where appropriate

5. Any electronic transfer methods across public space or cyberspace must be protected via encryption which has been certified under a NCSC (e.g. CAPS or CPA) or NCSC-endorsed scheme. Where this is not possible, the encryption method used must be approved IN ADVANCE by the Scottish Government prior to being used for the transfer any Scottish Government data.

6. Any portable removable media (including but not constrained to pen drives, memory sticks, CDs, DVDs, PDPs, USB devices) which handle, store or process in any way Scottish Government data to deliver and support the service, shall be under the configuration management of the (sub-)contractors providing the service, shall be necessary to deliver the service, and shall be full-disk encrypted using a product which has been certified under a NCSC (e.g. CAPS or CPA) or NCSC-endorsed scheme, failing that, approved for use by the Scottish Government's security contact.

7. All paper holding Scottish Government data must be securely protected whilst in the Service Provider's care and securely destroyed when no longer required using a cross-cutting shredder and/or a professional secure waste paper organisation.

8. Paper documents containing Scottish Government data shall be transmitted, both within and outside company premises in such a way as to make sure that no unauthorised person has access.

9. At the end of the contract or in the event of failure or obsoletion, all equipment holding Scottish Government data must be securely cleansed or destroyed using a NCSC approved product or method. Where this is not possible e.g. for legal or regulatory reasons, or technical reasons such as where there is storage area network (SAN) or shared backup tapes, then the Service Provider must protect the equipment until the time (which may be long after the end of the contract) when it can be securely cleansed or destroyed. In the case of Cloud storage, the NCSC Cloud Security Principles must be followed.

10. Access by Service Provider staff to Scottish Government data shall be confined to those individuals who have a "need-to-know" and whose access is essential for the purpose of their duties. All employees with direct or indirect access to Scottish Government data must be subject to pre-employment checks equal to the requirements of the HMG Baseline Personnel Security Standard (BPSS): Details of the standard are available at the HMG website https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.

11. All Service Provider employees who handle Scottish Government data must undertake annual awareness training in protecting information.

12. Any non-compliances with these Scottish Government conditions, or any suspected or actual breach of the confidentiality or integrity of Scottish Government data being handled in the course of providing this service, shall be immediately escalated to the Scottish Government by a method agreed by both parties.

13. The Service Provider shall ensure that any IT systems and hosting environments that are used to hold Scottish Government data being handled, stored or processed in the course of providing this service are periodically (at least annually) subject to independent, NCSC CHECK level, IT Health Checks (ITHC), and that the findings of those which are relevant to the service provided to the Scottish Government are shared with the Scottish Government and necessary remedial work carried out as per the timescales recommended by the independent test.

14. Where CHECK level testing is not permitted or possible, for example on a public cloud SAAS solution, the Service Provider will obtain and provide Scottish Government with documentary evidence of the most recent independent IT Health Check, will provide the results of said ITHC and provide the resulting remediation plan, including any actions proposed or taken.

15. The Service Provider will provide details of any proposal to store or host Scottish Government data outside the EU or to perform ICT management or support from

outside the UK and will not go ahead with such a proposal without prior agreement from the Scottish Government.

16. The Scottish Government reserves the right to audit the Service Provider with 24 hours' notice in respect to the Service Provider's compliance with the clauses contained in this Section.

17. The Service Provider will appoint a suitably qualified individual to act as a single point of contact on all security matters related to this contract, who will liaise with the primary point of contact within the Scottish Government, the Head of Digital Risk & Security for Social Security.

18. Where Personally Identifiable Information (PII) is involved, the Service Provider shall contractually enforce all of these Scottish Government Security conditions onto any third-party suppliers, sub-contractors or partners who could potentially access Scottish Government data in the course of providing this service.

19. Where no Personally Identifiable Information (PII) is involved, the Service Provider shall contractually enforce all of these Scottish Government Security conditions, with the exception of clause 1, where the required standard is the HMG Cyber Essentials certification or equivalent, onto any third-party suppliers, sub-contractors or partners who could potentially access Scottish Government data in the course of providing this service. Exceptions to this to be agreed in writing with the Scottish Government's Head of Digital Risk & Security – Social Security Programme.

## Social Security Programme

## Chief Digital Officer Division

# Hosting Platform Architecture Catalogue

## Enterprise Mobility Management

SSDCDO-HPA-0028-W2

Version: 0.1

# 1. Document Control

## 1.1. Document Information

| Doc Ref | Classification | Status | Author | Contact |
|---|---|---|---|---|
| TBC | | DRAFT | Hosting Platform Architecture | [redacted] |

## 1.2. Version Control/Approval

| Date | Updated By | Version | Reason for Change |
|---|---|---|---|
| 22/02/2018 | [redacted] | 0.1 | Initial Version |

## 1.3. Distribution

| Name | Role | Purpose |
|---|---|---|
| [redacted] | [redacted] | Approval |
| [redacted] | [redacted] | Approval |
| [redacted] | [redacted] | Review |
| [redacted] | [redacted] | Review |
| [redacted] | [redacted] | Review |
| [redacted] | [redacted] | Review |
| [redacted] | [redacted] | Review |

## 1.4. References

| Doc Ref | Title | Description |
|---|---|---|
| DR1 | Jamf Port Requirements | http://docs.jamf.com/9.9/casper-suite/jss-install-guide-windows/Ports.html |
| DR2 | Integrating with Apple's Device Enrollment Program (DEP) | https://www.jamf.com/jamf-nation/articles/359/integrating-with-apple-s-device-enrollment-program-dep |
| DR3 | TCP and UDP ports used by Apple software products | https://support.apple.com/en-us/HT202944 |

## 2. Contents

# 3. Background and Document Purpose

The Social Security Directorate (SSD) has chosen to adopt the DevOps software engineering culture and practice for the creation and management of the cloud hosting platform used by SSD business services.  The purpose of this document is to detail the method through which the workstations used by the DevOps team will be prepared for first-use, and how those workstations are to be managed thereafter.

## 4. Assumptions

- The DevOps team will use dedicated SSD owned workstations;
- SCOTS laptops will not be used for any DevOps tasks relating to the SSD Hosting Platform;
- The DevOps workstation specification is a latest generation (at time of writing) MacBook Pro 15" running MacOS High Sierra. 14 units of which were provisioned by SSD in February 2018;
- DevOps workstations must be considered to be managed devices in order to be provided with a network connection;
- DevOps workstations will not consume SCOTS credentials;
- Whilst within SG managed office estate, DevOps workstations will be able to connect to network provision via ethernet and WiFi;
- DevOps workstations will not be provisioned with direct access to AWS VPN Gateways. Connectivity will be provided via Hardware VPN Gateways located within SG / SSD Offices.
- DevOps workstations outwith SG real estate, rely upon VPN connectivity to reach SSD Office resources.

# 5. Overview

In order for a computer device to gain access to a network within a Scottish Government controlled building in any way, it must be considered to be a managed device. A device is typically considered managed if it is built to a standard image / configuration by a trusted department within a trusted/secure location. SCOTS Windows workstations (such as the HP Elitebook 820) are managed via a standardised windows installation image that includes standard software and configuration such as VPN clients and device identifying certificates.

*Figure 5.1 - Standard Scottish Government Laptop (HP Elitebook 820)*

At the time of writing, SSD will adopt the Apple MacBook Pro as their standard for workstations for DevOps engineers. As Scottish Government iTECS do not provide management support for Apple devices, SSD will implement a self-managed provisioning and management solution, typically referred to as Enterprise Mobility Management, which provides enforcement controls over the provision all SSD owned MacOS devices. In doing so, SSD will establish affected MacOS devices as managed workstation endpoints.

*Figure 5.2 – A Macbook Pro Workstation (similar to that used by SSD DevOps team)*

# 6. Enterprise Mobility Management

A variety of Enterprise Mobility Management (EMM) solutions exist for MacOS environments, each providing varying degrees of capability. The objective is to identify an appropriate EMM Solution for the SSD DevOps team. The DevOps team will use Apple MacOS devices and an EMM Solution should integrate with MDM capabilities offered by Apple, specifically the Apple Device Enrolment Programme.

## 6.1. Apple Device Enrolment Programme

Apple products can be registered at the time of purchase via a service offered by Apple called the Device Enrolment Program (DEP). From that moment on, even before the device is removed from its packaging, the device is 'bound' to a given organisation and is subject to appropriate configuration enforcement as an organisation sees fit. It is important that any EMM solution selected by SSD interfaces directly with the DEP so as to ensure streamlined management and policy enforcement.

## 6.2. EMM Requirements

SSD are specifically requiring the following functionality from an EMM solution:

- **DEP Integration –** Integration with Apple DEP for device management and policy enforcement;
- **Device Management –** The ability to enforce and manage the hardware and software configuration of a mobile device remotely;
- **Device Security –** The ability to enforce security policy upon a workstation and provide remote lockdown capabilities should a device be lost or compromised;
- **Application Management –** The ability for administrators to pre-authorise a catalogue of applications available for users to install, and a streamlined provisioning process for users to request additional software products.

## 6.3. Product Selection

Market research conducted by SSD solution architects, which included verification of findings against Gartner research and consultation with 3rd party organisations with requirements analogous to that of the SSD (such as MyGov.scot and SSD solution developers IBM), resulted in the identification and qualification of a suitable product. The selected product is Jamf Pro (https://www.jamf.com/products/jamf-pro/).

In combination with the Apple Device Enrolment Programme, Jamf Pro provides the most comprehensive, manageable and cost effective EMM solution for the DevOps workstation environment.

## 6.4. SSD EMM Solution

The SSD EMM Solution, which consists of a combination of Apple DEP, MDM Configuration capabilities and the JAMF Pro product, provides the following capabilities:

### 6.4.1. Device Management

SSD DevOps MacOS devices will be subject to enforcement of configuration, policy and profile settings including, but not limited to:

- **Recurring Check-In** – Devices are configured to communicate with Jamf services on a regular schedule to obtain available policies;
- **Startup Script** – The ability to enforce a startup script to execute upon workstation startup:
  - Log Computer Usage information (date/time of startup).
  - Check for policies triggered at startup.
  - Enable computer-level Managed Preferences.
  - Ensure SSH (Remote Login) is enabled on computers.
- **Login / Logout Hooks -** The Login/Logout Hooks settings allow for the creation of login and logout hooks on computers which can be used to perform the following actions:
  - Log Computer Usage information (username and date/time) at login and logout;
  - Check for policies triggered at login or logout;
  - Enable user-level and user-level enforced Managed Preferences at login;
  - Hide the Restore partition at login;
- **Security Settings –** Enforce control over the following settings:
  - Enable certificate-based authentication;
  - Enable push notifications;
  - Configure SSL certificate verification;
  - Specify the condition under which the checksum will be used to validate packages;
  - Specify a maximum clock skew between managed computers and the JSS host server.
- **Patch Management –** Patch management for Apple Updates consists of running Software Update on computers via policies. This process installs all updates available from Apple. Patch management for third-party macOS software titles consists of managing a software inventory and packaging updates for distribution via private distribution points for automatic deploying via smart groups and a policy;
- **License Management –** Store and track licenses for software throughout the SSD DevOps MacOS environment to easily access license information and monitor license compliance.

### 6.4.2. Device Security

SSD DevOps MacOS devices will be subject to enforcement of security controls and measures including but not limited to:

- **SSL Certificate Verification –** Configuring the SSL Certificate Verification setting ensures that computers only communicate with a host server that has a valid SSL certificate. This prevents computers from communicating with an imposter server and protects against man-in-the-middle attacks.
- **Disk Encryption** (Keys are securely stored within JAMF Pro infrastructure)
- **Enforcement of MDM Policy and Profiles**. Local MacOS users will be unable to remove any MDM policies / profiles applied.
- **Client Certificate Enforcement and Renewal –** Client Certificates used for client identification and authorisation are issued from centrally managed services;
- **Remote device management –** Administrators have the capability to remotely access a device to perform administrative tasks upon it**;**
- **Remote device wipe –** Administrators can remotely wipe a device should it become compromised or lost**;**
- **Device location detection –** Administrators are able to physically locate devices

### 6.4.3. Application Management

SSD DevOps MacOS devices will be subject to controls over what apps can be installed on the devices. The methods of software installation include but are not limited to:

- SSD will be able to distribute Mac App Store apps and eBooks purchased through Apple's Volume Purchase Program (VPP) to computers and users via VPP-managed distribution;
- VPP content searches allowing detailed search criteria to search Mac App Store apps;
- VPP content search results can be exported for later analysis;
- SSD are able control how and when Mac App Store apps are updated and on which computers that were distributed using VPP-managed distribution. There are two possible update modes:
  - **Enable automatic app updates –** Enable automatic app updates for all Mac App Store apps. This update happens once a day.
  - **Force apps to update –** Force all Mac App Store apps to update immediately on computers if there are updates available.
- Deployment of custom application packages and MacOS installers

### 6.4.4. Support

To help ensure customer success, all sales of Jamf Pro include new customer primer sessions and a personal training and implementation engagement called Jamf JumpStart. As depicted in Figure 6.1 below, through remote and on-site sessions, SSD will be equipped with all the tools necessary to get the most out of the product and begin implementing solutions to the challenges within the Apple management ecosystem.

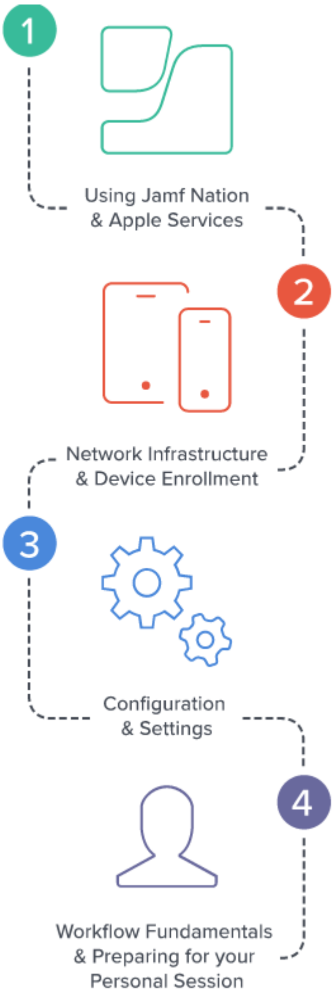


*Figure 6.1 - Jamf Setup Flow*

During the primer sessions, SSD participate in a series of four workshops with a Jamf expert. This allows both novice and experienced Apple users to start using the solution and receive personalised support. The workshops include:

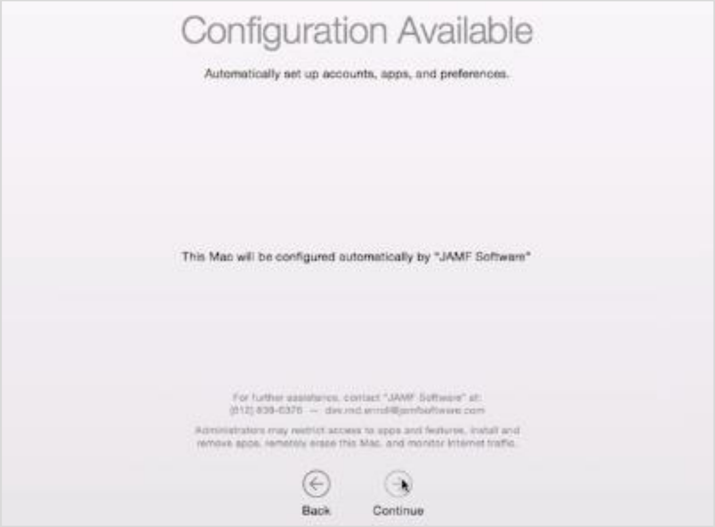
- Using Jamf Nation & Apple Services
- Network Infrastructure & Device Enrolment
- Configuration & Settings
- Workflow Fundamentals & Preparing for your personal session

During the personalized Jamf JumpStart session, a Jamf expert will with SSD to configure and integrate Jamf Pro seamlessly into the overall EMM solution. Through a hands-on approach, the Jamf expert will provide workflow recommendations, an overview of support resources available, and additional training and certification options.  The following list is a summary of the 2-day onsite workshop for MacOS:

- One 2-day onsite engagement
- macOS training for the primary Jamf Pro administrator(s) in your organization
- Set up and configure Jamf Pro for macOS management

## 6.5. DevOps User experience

Devices under the control of the SSD EMM solution will have the configuration, policy and profiles defined applied at initial setup, as configured by administrators. When a device is switched on for the first time, or reset back to factory defaults, it will communicate with Apple DEP services, and be recognised as a device is under control of EMM, informing the user as they progress through the setup wizard as depicted in Figure 6.2 below.



Configuration Available

Automatically set up accounts, apps, and preferences.

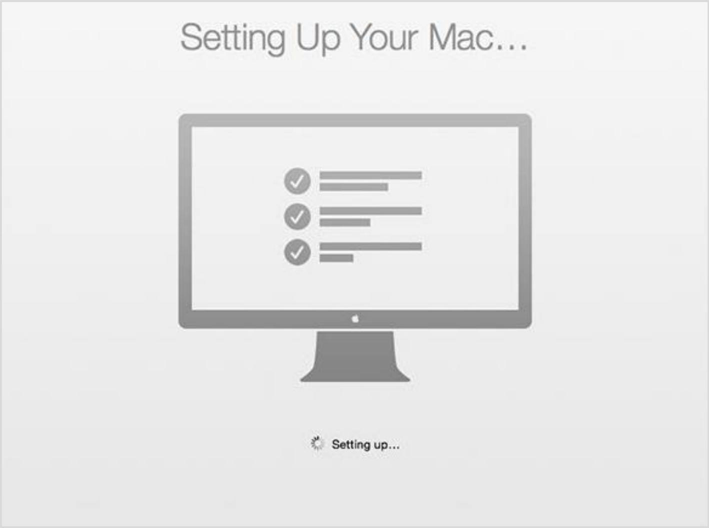
This Mac will be configured automatically by "JAMF Software"

For further assistance, contact "JAMF Software" at:
(612) 639-0376 — dev.mdi.enroll@jamfsoftware.com

Administrators may restrict access to apps and features, install and remove apps, remotely erase this Mac, and monitor Internet traffic.

*Figure 6.2 - MacOS Setup Wizard informing end user that the computer is subject to automatic configuration*

Upon conclusion of the setup wizard, the MacOS device is configured with all configuration, policy and profiles (See Figure 6.3 below).



Setting Up Your Mac…

Setting up…

*Figure 6.3 - MacOS Setup Wizard automatically applying configuration, policy and profiles as defined in DEP*

Once configured, the DevOps team will be able to install applications

# 7. Device Provisioning

There are a number of methods for the SSD EMM solution to provision an Apple device used by SSD DevOps team. These include:

1. Machine Imaging;
2. Network Scan;
3. User Initiated;
4. Zero-Touch (JAMF / Apple Device Enrolment Program).

### Machine Imaging

The most traditional option for device provisioning is to build a standardised machine image which is applied to every new machine, typically within a secure build room. Whilst this option provides administrators with the enforce initial standardisation of workstations it introduces considerable management overheads including:

- Requirement for administrative resource and physical build time;
- Multiple image versions must be maintained;
- Support issues must be managed;

### Network Scan

The proposed SSD EMM solution is capable of enrolling devices into the EMM managed estate through their discovery via a network scan. This however requires the connection of untrusted devices to a trusted corporate network. This requirement presents an unacceptable risk of exposure to corporate networks and therefore is not an appropriate solution.

### User Initiated

The proposed SSD EMM solution is capable of allowing users to manually enrol their device into the EMM managed estate via a web interface and agent installation. This method involves an untrusted device being connected to a trusted corporate network and therefore, for the same reasons as Network Scan, this requirement presents an unacceptable risk of exposure to corporate networks and therefore is not an appropriate solution.

### Zero-Touch enrolment via JAMF and Apple Device Enrolment Programme (DEP)

A feature presented by the proposed SSD EMM solution is the ability for Mac devices to be pre-registered, at point of purchase, upon a trusted Device Enrolment Programme register operated by Apple. This enables the pre-configuration of devices, with SSD controlled configuration, policies and profiles, when they are first turned on, or when they rebuilt.

This results in a zero-touch enrolment capability that requires little or no involvement from device administrators during device setup – users can be handed a device and can set up the machine without admin involvement. Importantly, because the machines are known to DEP, which is communicated with during setup, there is no way for the user to bypass the application of SSD configuration, policies and profiles.

As an alternative, should users not to be trusted to perform initial device setup, device administrators could perform the initial setup from within a secure build room using an isolated internet connection.

## 7.1. Selected Method for New Device Provisioning

Zero Touch Enrolment is the preferred method of new device provisioning, allowing users to invoke automated device provisioning and setup without administrative involvement. However, administrators may perform the same tasks within a secure build room environment should infrastructure and security requirements stipulate this as necessary.

## 7.2. Provisioning Process

The objective of the SSD EMM provision is to establish SSD DevOps devices as managed and provisioned devices. This is achieved through the utilisation of services offered by both JAMF Pro software and Apple Corporation DEP. These services are combined to enable the provisioning flow defined in the table below:

*Table 7.1 - EMM Device Provisioning Stages*

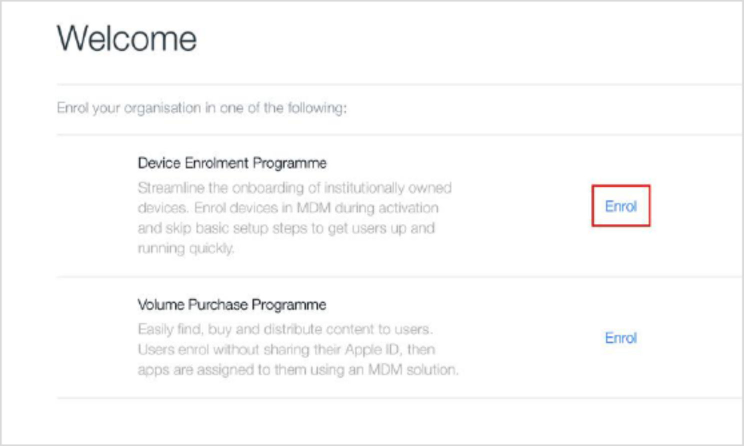
| Step | Provision Stage | Description of Stage | Device Status |
|---|---|---|---|
| **1** | New | **New Purchase / Boxed**<br>Serial and Physical MAC Address of every mac device purchased is registered by the supplier against the SSD Apple DEP account. | Known |
| **2** | Issued | **Laptop issued to DevOps Engineer**<br>1. Device is turned on;<br>2. Connected to WiFi (for example: SCOTS Guest wifi);<br>3. Apple setup wizard securely communicates with Apple Corp registration services;<br>4. SSD Configuration and Profiles are downloaded and applied immediately (including Acceped Wifi SSIDs, Encryption, Client Certificates, and JAMF MDM Configuration) | Managed |

| Step | Provision Stage | Description of Stage | Device Status |
|---|---|---|---|
| **3** | Ready | **Laptop connects to SSD Network (WiFi/Ethernet)**<br>Laptop connects to SSD network and authorises itself using trusted client certificates. The user may then downloads apps from the trusted SSD application store | Provisioned |

## 7.3. Provisioning Prerequisites

### 7.3.1. Apple DEP Registration and Configuration

Registration with the Apple Device Enrolment Programme is required as part of the proposed EMM solution. This is achieved by registering on Apple's website at https://deploy.apple.com/ with a corporate Apple ID (may need to be created).



Welcome

Enrol your organisation in one of the following:

Device Enrolment Programme

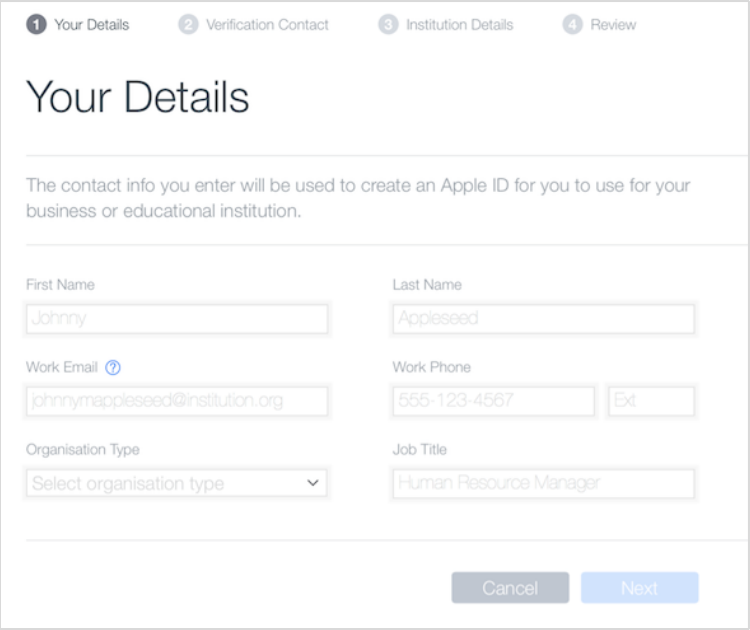
Streamline the onboarding of institutionally owned devices. Enrol devices in MDM during activation and skip basic setup steps to get users up and running quickly.

Volume Purchase Programme

Easily find, buy and distribute content to users. Users enrol without sharing their Apple ID, then apps are assigned to them using an MDM solution.

*Figure 7.1 - Apple Device Enrolment Programme Registration*

To complete the registration process, a new Apple ID will get created. The first contact form will ask you for an email address (amongst other things) which will be used to automatically create a new Apple ID for administration:



❶ Your Details ② Verification Contact ③ Institution Details ④ Review

Your Details

The contact info you enter will be used to create an Apple ID for you to use for your business or educational institution.

First Name: Johnny

Last Name: Appleseed

Work Email ⓘ: johnnymappleseed@institution.org

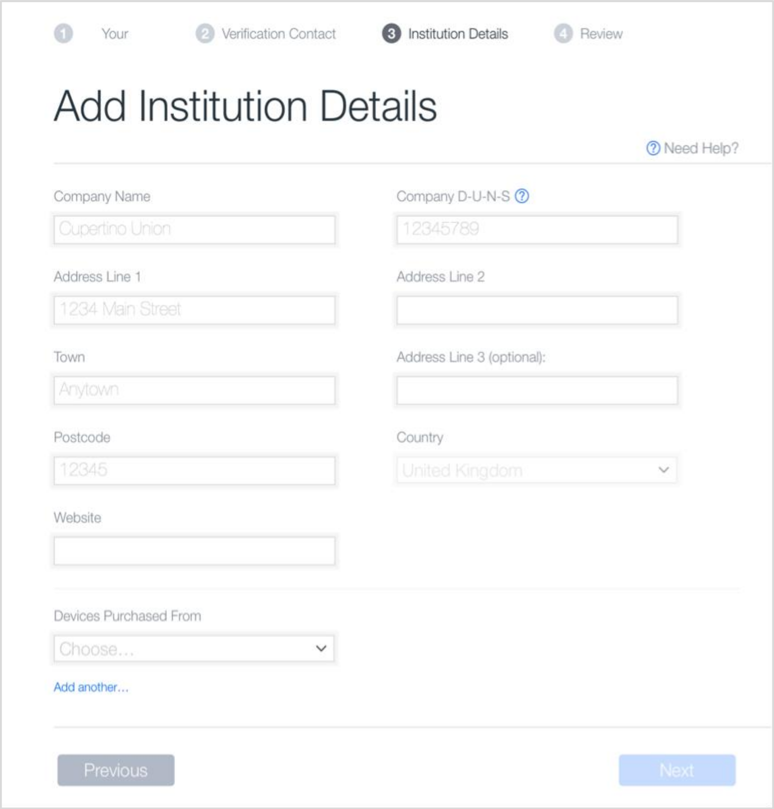
Work Phone: 555-123-4567 Ext

Organisation Type: Select organisation type

Job Title: Human Resource Manager

*Figure 7.2 - Apple Device Enrolment Programme - Administrator Details (per admin)*

A new Apple ID must be created for each administrator, using their @gov.scot domain email address. Once the Apple ID has been verified (via one-time code sent via email), the next step is to provide institutional information:



① Your ② Verification Contact ❸ Institution Details ④ Review

Add Institution Details

ⓘ Need Help?

Company Name: Cupertino Union

Company D-U-N-S ⓘ: 12345789

Address Line 1: 1234 Main Street

Address Line 2:

Town: Anytown

Address Line 3 (optional):

Postcode: 12345

Country: United Kingdom

Website:

Devices Purchased From: Choose...

Add another...

*Figure 7.3 - Apple Device Enrolment Programme - Institution Details*

### Company D-U-N-S

This is an identification number for businesses regulated by Dun & Bradstreet (D&B) that assigns a unique numeric identifier, referred to as a “DUNS number” to a single business entity.

### Devices Purchased From

The identification of the supplier from which the devices were purchased.  This It will be used to associate the serial numbers of any devices you purchase with your DEP account. Multiple sources, including Apple and third-party resellers, can be identified, as long as they are official Apple resellers and registered with the DEP service.

Upon submission of the application Apple will process the registration.

# 8. EMM Architecture

## 8.1. Server Architecture

Two instances of JAMF Pro are to be established within the hosting environment:

- Test Instance;
- Live Instance.

All configuration, policy and profile changes will be tested and evaluated using the testing JAMF Instance with effect against a limited scope of MacOS workstations (test workstations).

Version and change control for JAMF Configurations is to be established, through storage of configuration versions within the SSD Source Version Control System (GitLab).

### 8.1.1. Distribution Points

Distribution points are servers used to host files for distribution to computers and mobile devices. Software Packages, Scripts and In-house apps can be distributed from a distribution point using the Jamf:

The Jamf Pro supports three types of distribution points:

- File share distribution points
- A cloud distribution point
- Jamf Distribution Server (JDS) instances

Any combination of these types of distribution points can be used.

By default, the first distribution point added to the Jamf Software Server (JSS) is the master distribution point. The master distribution point is used by all other distribution points as the authoritative source for all files during replication. The master distribution point can be changed at any time.

When planning distribution point infrastructure, it is important to understand the differences between each type of distribution point. Table 11.1 explains the key differences.

The SSD EMM Solution will utilise two distribution points, namely:

- On Premise Jamf Distribution Server (JDS)
- Cloud Distribution point using Amazon AWS S3 Storage Bucket

The On-Premise distribution server (JDS) is configured as the master distribution source and will therefore be the source from which any other distribution sources synchronise.

## 8.2. EMM Server Architecture Diagram

### 8.2.1. Day 1

Diagram 8.1 depicts network connectivity for ‘day 1’ of operations.

[redacted] [redacted]

[redacted]

### 8.2.2. Day 2

Diagram 8.2 depicts network connectivity for ‘day 2’ of operations.

[redacted]

[redacted]

# 9. EMM Configuration

## 9.1. Linking MDM System (Jamf) to DEP

The next step is to link the DEP account to the JAMF Pro MDM system.

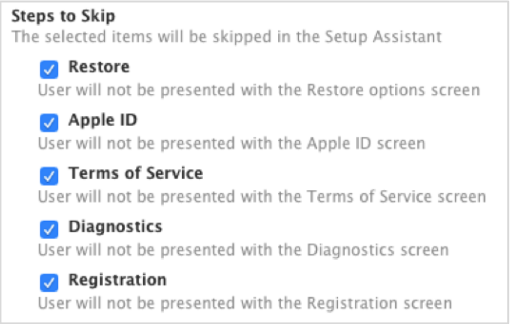
This involves the following process:

- Select Device Enrolment Program from the Global Management screen and download the Public Key;
- Use the public key to add Jamf Pro to the Apple DEP portal. Adding the server to the DEP portal provides a Server Token File;
- Take the Server Token File and use it to add the account to the JSS;

Once JAMF has been registered within the DEP portal, newly purchased devices are automatically enrolled into the MDM.

## 9.2. Configure PreStage Enrolments

A pre-stage enrolment is the configuration policy that is applied when a device is set up (first switched on / Operating System Reset). Included in the configurable options is the ability to determine which screens are displayed during initial workstation configuration:



**Steps to Skip**
The selected items will be skipped in the Setup Assistant

☑ **Restore**
User will not be presented with the Restore options screen

☑ **Apple ID**
User will not be presented with the Apple ID screen

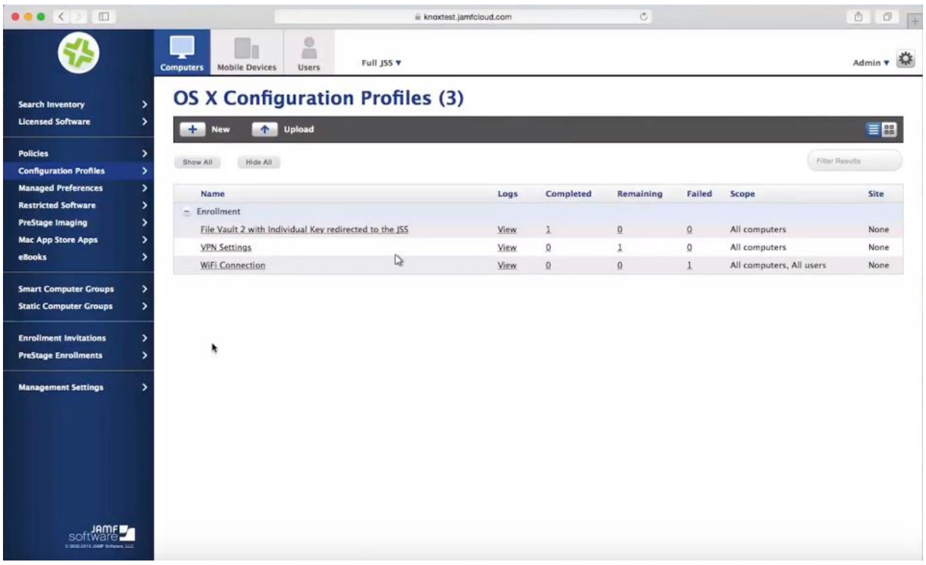
☑ **Terms of Service**
User will not be presented with the Terms of Service screen

☑ **Diagnostics**
User will not be presented with the Diagnostics screen

☑ **Registration**
User will not be presented with the Registration screen

*Figure 11 - MacOS Setup / Configuration Wizard steps*

The configuration policies and profiles are defined within the JAMF Pro service, as depicted in Figure 9.2, such as policies regarding File Encryption, VPN and WiFi settings.



OS X Configuration Profiles (3)

| Name | Logs | Completed | Remaining | Failed | Scope | Site |
|---|---|---|---|---|---|---|
| − Enrollment | | | | | | |
| File Vault 2 with Individual Key redirected to the JSS | View | 1 | 0 | 0 | All computers | None |
| VPN Settings | View | 0 | 1 | 0 | All computers | None |
| WiFi Connection | View | 0 | 0 | 1 | All computers, All users | None |

*Figure 9.2 - Example MacOS Configuration Profiles*

# 10. Application Deployments

At the time of writing, a comprehensive list of applications required by the DevOps team are yet unidentified.  The applications and services detailed within this section are however known to be fundamentally required in order to provide capabilities necessary for DevOps team to operate.

## 10.1. User Account Credential Management

The SSD hosting platform is defining a network security policy that details the requirements of user account privilege and credential management within the SSD Hosting Platform environment.  It is the ambition of the Hosting platform architecture team to find a solution to extending the network security policy enforcement beyond the Hosting Platform, onto the managed MacOS environment.

Through use of a product called NoMAD, SSD DevOps Engineers are able to utilise their SSD AWS Active Directory credentials for single sign-on against all SSD AWS Services using secure Kerberos authentication.

Further functionality includes:

- Use SSD AWS AD credentials for single sign-on for all services using Kerberos authentication.
- Automatic and manual retrieval of X509 identities from existing Windows Certificate Authorities.
- One click access to Jamf Pro self-service applications.
- Syncing AD password to local MacOS accounts, including keeping the user’s local keychain and FileVault passwords in sync.
- Enforcement of password expirations and automated warning about impending password expirations.

# 11. Appendix A

## 11.1. Comparison of Jamf distribution point types

*Table 11.1 - Comparison of Jamf distribution point types*

| | File Share | Cloud | JDS Instance |
|---|---|---|---|
| **Description** | Standard server that is configured to be a distribution point | Distribution point that uses one of the following content delivery networks (CDNs) to host files:<br>• Rackspace Cloud Files<br>• Amazon Web Services<br>• Akamai | Distribution point that is managed by the JSS, similar to a computer or mobile device |
| **Maximum Number per JSS** | Unlimited | One | Unlimited |
| **Server/Platform Requirements** | Any server with an Apple Filing Protocol (AFP) or Server Message Block (SMB) share | None | Mac or Linux |
| **Protocol** | AFP, SMB, HTTP, or HTTPS | HTTPS | HTTPS |
| **Ports** | AFP: 548<br>SMB: 139<br>HTTP: 80<br>HTTPS: 443 | 443 | 443 |
| **Authentication Options** | • AFP or SMB:<br>o No authentication<br>o Username and password<br>• HTTP or HTTPS:<br>o No authentication<br>o Username and password<br>• Certificate-based authentication | None | No authentication<br>Certificate-based authentication |
| **Files that Can Be Hosted** | • Packages<br>• Scripts | • Packages<br>• In-house apps<br>• In-house eBooks<br>Note: If you use the cloud distribution point, scripts are stored in the jamfsoftware database. | • Packages<br>• In-house apps<br>• In-house eBooks<br>Note: If you use one or more JDS instances, scripts are stored in the |

| | File Share | Cloud | JDS Instance |
|---|---|---|---|
| | | | jamfsoftware database. |
| **Parent-Child Capabilities** | No | No | Yes |
| **File Replication Method** | Replication to file share distribution points must be initiated from Casper Admin. | Replication to a cloud distribution point must be initiated from Casper Admin. | Replication to root JDS instances must be initiated from JSS Admin.<br>Replication to non-root JDS instances happens automatically and immediately. |
| **Selective Replication** | Not available when replicating to file share distribution points. | Available when replicating to a cloud distribution point if the master distribution point is a JDS instance or file share distribution point. The files for replication must be specified in the JSS and the replication initiated from Jamf Admin. | Not available when replicating to root JDS instances.<br>Available when replicating to non-root JDS instances. The files for replication must be specified in the JSS. The replication from non-root parent to child instances is initiated on check in with the JSS. |

## 11.2. Apple Device Management TCP Port Requirements

| Port | Used for | Direction |
|---|---|---|
| **22** | The standard port for SSH (known as remote login in OS X). Default port used by Jamf Remote and Recon to connect to computers. | Outbound from Jamf Remote and Recon, and inbound to computers |
| **80** | The standard port for HTTP. When you use HTTP to distribute files from a file share distribution point, they are downloaded on this port. | Inbound to the distribution point, and outbound from computers |
| **443*** | The standard port for HTTPS. When you use HTTPS to distr bute files from a file share distribution point, they are downloaded on this port. The cloud distribution point and JDS instance also communicates on this port.<br>In addition, this port is used for the following:<br>• Connect the JSS to the JAMF Push Proxy.<br>• Required for MDM-capable computers to communicate with Apple Push Notification service (APNs).<br>• Connect to Apple's Device Enrollment Program (DEP) and Volume Purchase Program (VPP). | Inbound to the distribution point, and outbound from the JSS, computers, and mobile devices |

| Port | Used for | Direction |
|---|---|---|
| | **Note:** Apple could change this port without JAMF Software knowledge. | |
| **548** | The standard port for Apple File Protocol (AFP). If you use an AFP share to distribute files from a file share distribution point, computers mount the AFP share on this port. | Inbound to the share, and outbound from computers |
| **3306** | The default port used by the JSS to connect to MySQL. | Outbound from the JSS, and inbound to MySQL |
| **8443** | The SSL port for the JSS. Default port used by applications and computers and mobile devices to connect to the JSS. | Inbound to the JSS, and outbound from computers and mobile devices |
| **25** | The standard port for SMTP. The JSS connects to an SMTP server to send email notifications to JSS users. | Outbound from the JSS, and inbound to the SMTP server |
| **139** | If you use an SMB share to distribute files from a file share distr bution point, computers mount the SMB share on this port. | Inbound to the share, and outbound from computers |
| **389** | The standard port for LDAP. Any LDAP connections—even those coming from other applications—go through the JSS. This means that only the JSS connects to your LDAP server. | Outbound from the JSS, and inbound to the LDAP server |
| **636** | The standard port for LDAPS. Any LDAP connections—even those coming from other applications—go through the JSS. This means that only the JSS connects to your LDAP server. | Outbound from the JSS, and inbound to the LDAP server |
| **445** | If you have an SMB client, such as "DAVE", installed on computers, they may mount the SMB share on this port. | Inbound to the share, and outbound from computers |
| **514** | The default port used by the JSS to write to Syslog servers. | Outbound from the JSS, and inbound to Syslog servers |
| **2195*** | The port used to send messages from the JSS to APNs. | Outbound from the JSS, and inbound to the APNs server |
| **2196*** | The port used by the JSS to connect to APNs for feedback. | Outbound from the JSS, and inbound to the APNs server |
| **5223*** | The port used to send messages from APNs to the computers and iOS devices in your network. | Outbound from computers and iOS devices, and inbound to the APNs server |
| **5228** | The port used to send messages from Google Cloud Messaging (GCM) to the personally owned Android devices in your network. | Outbound from Android devices, and inbound to the GCM server |

| Port | Used for | Direction |
|---|---|---|
| **8080** | The HTTP port for the JSS on Linux and Windows platforms. Although it is available, applications do not connect to this port unless the defaults are overridden. | N/A |
| **9006** | The HTTP port for the JSS on the Mac platform. Although it is available, applications do not connect to this port unless the defaults are overridden. | N/A |

* Ports 443, 2195, 2196, and 5223 must be open outbound and inbound to the 17.0.0.0/8 address block in order for computers and iOS devices to communicate with APNs.

## 11.3. Ports used by Apple products

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| 7 | TCP/UDP | echo | 792 | echo | — |
| 20 | TCP | File Transport Protocol (FTP) | 959 | ftp-data | — |
| 21 | TCP | FTP control | 959 | ftp | — |
| 22 | TCP | Secure Shell (SSH), SSH File Transfer Protocol (SFTP), and Secure copy (scp) | 4253 | ssh | Xcode Server (hosted and remote Git+SSH; remote SVN+SSH) |
| 23 | TCP | Telnet | 854 | telnet | — |
| 25 | TCP | Simple Mail Transfer Protocol (SMTP) | 5321 | smtp | Mail (sending email); iCloud Mail (sending email) |
| 53 | TCP/UDP | Domain Name System (DNS) | 1034 | domain | — |
| 67 | UDP | Bootstrap Protocol Server (BootP, bootps) | 951 | bootps | NetBoot via DHCP |
| 68 | UDP | Bootstrap Protocol Client (bootpc) | 951 | bootpc | NetBoot via DHCP |
| 69 | UDP | Trivial File Transfer Protocol (TFTP) | 1350 | tftp | — |

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| 79 | TCP | Finger | 1288 | finger | — |
| 80 | TCP | Hypertext Transfer Protocol (HTTP) | 2616 | http | World Wide Web, FaceTime, iMessage, iCloud, QuickTime Installer, Maps, iTunes U, Apple Music, iTunes Store, Podcasts, Internet Radio, Software Update (OS X Lion or earlier), Mac App Store, RAID Admin, Backup, Calendar, WebDAV, Final Cut Server, AirPlay, macOS Internet Recovery, Profile Manager, Xcode Server (Xcode app, hosted and remote Git HTTP, remote SVN HTTP) |
| 88 | TCP | Kerberos | 4120 | kerberos | Kerberos, including Screen Sharing authentication |
| 106 | TCP | Password Server (unregistered use) | — | 3com-tsmux | macOS Server Password Server |
| 110 | TCP | Post Office Protocol (POP3),<br>Authenticated Post Office Protocol (APOP) | 1939 | pop3 | Mail (receiving email) |
| 111 | TCP/UDP | Remote Procedure Call (RPC) | 1057, 1831 | sunrpc | Portmap (sunrpc) |
| 113 | TCP | Identification Protocol | 1413 | ident | — |
| 119 | TCP | Network News Transfer Protocol (NNTP) | 3977 | nntp | Apps that read newsgroups. |
| 123 | UDP | Network Time Protocol (NTP) | 1305 | ntp | Date & Time preferences, network time server synchronization, Apple TV network time server sync |
| 137 | UDP | Windows Internet Naming Service (WINS) | — | netbios-ns | — |
| 138 | UDP | NETBIOS Datagram Service | — | netbios-dgm | Windows Datagram Service, Windows Network Neighborhood |
| 139 | TCP | Server Message Block (SMB) | — | netbios-ssn | Microsoft Windows file and print services, such as Windows Sharing in macOS |

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| 143 | TCP | Internet Message Access Protocol (IMAP) | 3501 | imap | Mail (receiving email) |
| 161 | UDP | Simple Network Management Protocol (SNMP) | 1157 | snmp | — |
| 192 | UDP | OSU Network Monitoring System | — | osu-nms | AirPort Base Station PPP status or discovery (certain configurations), AirPort Admin Utility, AirPort Express Assistant |
| 311 | TCP | Secure server administration | — | asip-webadmin | Server app, Server Admin, Workgroup Manager, Server Monitor, Xsan Admin |
| 312 | TCP | Xsan administration | — | vslmp | Xsan Admin (OS X Mountain Lion v10.8 and later) |
| 389 | TCP | Lightweight Directory Access Protocol (LDAP) | 4511 | ldap | Apps that look up addresses, such as Mail and Address Book |
| 427 | TCP/UDP | Service Location Protocol (SLP) | 2608 | svrloc | Network Browser |
| 443 | TCP | Secure Sockets Layer (SSL or HTTPS) | 2818 | https | TLS websites, iTunes Store, Software Update (OS X Mountain Lion and later), Spotlight Suggestions, Mac App Store, Maps, FaceTime, Game Center, iCloud authentication and DAV Services (Contacts, Calendars, Bookmarks), iCloud backup and apps (Calendars, Contacts, Find My iPhone, Find My Friends, Mail, iMessage, Documents & Photo Stream, iCloud Key Value Store (KVS), iPhoto Journals, AirPlay, macOS Internet Recovery, Profile Manager, Back to My Mac, Dictation, Siri (iOS), Xcode Server (hosted and remote Git HTTPS, remote SVN HTTPS, Apple Developer registration), Push notifications (if necessary) |
| 445 | TCP | Microsoft SMB Domain Server | — | microsoft-ds | — |
| 464 | TCP/UDP | kpasswd | 3244 | kpasswd | — |

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| 465 | TCP | Message Submission for Mail (Authenticated SMTP) | | smtp (legacy) | Mail (sending mail) |
| 500 | UDP | ISAKMP/IKE | 2408 | isakmp | macOS Server VPN service, Back to My Mac |
| 500 | UDP | Wi-Fi Calling | 5996 | IKEv2 | Wi-Fi Calling |
| 514 | TCP | shell | — | shell | — |
| 514 | UDP | Syslog | — | syslog | — |
| 515 | TCP | Line Printer (LPR), Line Printer Daemon (LPD) | — | printer | Printing to a network printer, Printer Sharing in macOS |
| 532 | TCP | netnews | — | netnews | — |
| 548 | TCP | Apple Filing Protocol (AFP) over TCP | — | afpovertcp | AppleShare, Personal File Sharing, Apple File Service |
| 554 | TCP/UDP | Real Time Streaming Protocol (RTSP) | 2326 | rtsp | AirPlay, QuickTime Streaming Server (QTSS), streaming media players |
| 587 | TCP | Message Submission for Mail (Authenticated SMTP) | 4409 | submission | Mail (sending mail), iCloud Mail (SMTP authentication) |
| 600–1023 | TCP/UDP | Mac OS X RPC-based services | — | ipcserver | NetInfo |
| 623 | UDP | Lights-Out-Monitoring | — | asf-rmcp | Lights Out Monitoring (LOM) feature of Intel-based Xserve computers, Server Monitor |
| 625 | TCP | Open Directory Proxy (ODProxy) (unregistered use) | — | dec_dlm | Open Directory, Server app, Workgroup Manager; Directory Services in OS X Lion or earlier<br>This port is registered to DEC DLM |
| 626 | TCP | AppleShare Imap Admin (ASIA) | — | asia | IMAP administration (Mac OS X Server v10.2.8 or earlier) |

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| 626 | UDP | serialnumberd (unregistered use) | — | asia | Server serial number registration (Xsan, Mac OS X Server v10.3 – v10.6) |
| 631 | TCP | Internet Printing Protocol (IPP) | 2910 | ipp | macOS Printer Sharing, printing to many common printers |
| 636 | TCP | Secure LDAP | — | ldaps | — |
| 660 | TCP | Server administration | — | mac-srvr-admin | Server administration tools for Mac OS X Server v10.4 or earlier, including AppleShare IP |
| 687 | TCP | Server administration | — | asipregistry | Server administration tools for Mac OS X Server v10.6 or earlier, including AppleShare IP |
| 749 | TCP/UDP | Kerberos 5 admin/changepw | — | kerberos-adm | — |
| 985 | TCP | NetInfo Static Port | — | — | — |
| 993 | TCP | Mail IMAP SSL | — | imaps | iCloud Mail (SSL IMAP) |
| 995 | TCP/UDP | Mail POP SSL | — | pop3s | — |
| 1085 | TCP/UDP | WebObjects | — | webobjects | — |
| 1099, 8043 | TCP | Remote RMI and IIOP Access to JBOSS | — | rmiregistry | — |
| 1220 | TCP | QT Server Admin | — | qt-serveradmin | Administration of QuickTime Streaming Server |
| 1640 | TCP | Certificate Enrollment Server | — | cert-responder | Profile Manager in macOS Server 5.2 and earlier |
| 1649 | TCP | IP Failover | — | kermit | — |
| 1701 | UDP | L2TP | — | l2f | macOS Server VPN service |
| 1723 | TCP | PPTP | — | pptp | macOS Server VPN service |
| 1900 | UDP | SSDP | — | ssdp | Bonjour, Back to My Mac |

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| 2049 | TCP/UDP | Network File System (NFS) (version 3 and 4) | 3530 | nfsd | — |
| 2195 | TCP | Apple Push Notification Service (APNS) | — | — | Push notifications |
| 2196 | TCP | Apple Push Notification Service (APNS) | — | — | Feedback service |
| 2336 | TCP | Mobile account sync | — | appleugcontrol | Home directory synchronization |
| 3004 | TCP | iSync | — | csoftragent | — |
| 3031 | TCP/UDP | Remote AppleEvents | — | eppc | Program Linking, Remote Apple Events |
| 3283 | TCP/UDP | Net Assistant | — | net-assistant | Apple Remote Desktop 2.0 or later (Reporting feature), Classroom app (command channel) |
| 3284 | TCP/UDP | Net Assistant | — | net-assistant | Classroom app (document sharing) |
| 3306 | TCP | MySQL | — | mysql | — |
| 3478–3497 | UDP | — | — | nat-stun-port - ipether232port | FaceTime, Game Center |
| 3632 | TCP | Distributed compiler | — | distcc | — |
| 3659 | TCP/UDP | Simple Authentication and Security Layer (SASL) | — | apple-sasl | macOS Server Password Server |
| 3689 | TCP | Digital Audio Access Protocol (DAAP) | — | daap | iTunes Music Sharing, AirPlay |
| 3690 | TCP/UDP | Subversion | — | svn | Xcode Server (anonymous remote SVN) |
| 4111 | TCP | XGrid | — | xgrid | — |
| 4398 | UDP | — | — | — | Game Center |

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| 4488 | TCP | Apple Wide Area Connectivity Service | | awacs-ice | Back To My Mac |
| 4500 | UDP | IPsec NAT Traversal | 4306 | ipsec-msft | macOS Server VPN service, Back to My Mac.<br>Configuring Back to My Mac on an AirPort Base Station or AirPort Time Capsule in NAT mode impedes connectivity to a macOS Server VPN service behind that NAT. |
| 4500 | UDP | Wi-Fi Calling | 5996 | IKEv2 | Wi-Fi Calling |
| 5003 | TCP | FileMaker - name binding and transport | — | fmpro-internal | — |
| 5009 | TCP | (unregistered use) | — | winfs | AirPort Utility, AirPort Express Assistant |
| 5100 | TCP | — | — | socalia | macOS camera and scanner sharing |
| 5222 | TCP | XMPP (Jabber) | 3920 | jabber-client | Jabber messages |
| 5223 | TCP | Apple Push Notification Service (APNS) | — | — | iCloud DAV Services (Contacts, Calendars, Bookmarks), Push notifications, FaceTime, iMessage, Game Center, Photo Stream, Back to My Mac |
| 5297 | TCP | — | — | — | Messages (local traffic) |
| 5350 | UDP | NAT Port Mapping Protocol Announcements | — | — | Bonjour, Back to My Mac |
| 5351 | UDP | NAT Port Mapping Protocol | — | nat-pmp | Bonjour, Back to My Mac |
| 5353 | UDP | Multicast DNS (MDNS) | 3927 | mdns | Bonjour, AirPlay, Home Sharing, Printer Discovery, Back to My Mac |
| 5432 | TCP | PostgreSQL | — | postgresql | Can be enabled manually in OS X Lion Server (previously enabled by default for ARD 2.0 Database) |
| 5897–5898 | UDP | (unregistered use) | — | — | xrdiags |

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| 5900 | TCP | Virtual Network Computing (VNC) (unregistered use) | — | vnc-server | Apple Remote Desktop 2.0 or later (Observe/Control feature) Screen Sharing (Mac OS X 10.5 or later) |
| 5988 | TCP | WBEM HTTP | — | wbem-http | Apple Remote Desktop 2.x See also dmtf.org/standards/wbem. |
| 6970–9999 | UDP | — | — | — | QuickTime Streaming Server |
| 7070 | TCP | RTSP (unregistered use), Automatic Router Configuration Protocol (ARCP) | — | arcp | QuickTime Streaming Server (RTSP) |
| 7070 | UDP | RTSP alternate | — | arcp | QuickTime Streaming Server |
| 8000–8999 | TCP | — | — | irdmi | Web service, iTunes Radio streams |
| 8005 | TCP | Tomcat remote shutdown | — | — | — |
| 8008 | TCP | iCal service | — | http-alt | Mac OS X Server v10.5 or later |
| 8080 | TCP | Alternate port for Apache web service | — | http-alt | Also JBOSS HTTP in Mac OS X Server 10.4 or earlier |
| 8085–8087 | TCP | W ki service | — | — | Mac OS X Server v10.5 or later |
| 8088 | TCP | Software Update service | — | radan-http | Mac OS X Server v10.4 or later |
| 8089 | TCP | Web email rules | — | — | Mac OS X Server v10.6 or later |
| 8096 | TCP | Web Password Reset | — | — | Mac OS X Server v10.6.3 or later |
| 8170 | TCP | HTTPS (web service/site) | — | — | Podcast Capture/podcast CLI |
| 8171 | TCP | HTTP (web service/site) | — | — | Podcast Capture/podcast CLI |
| 8175 | TCP | Pcast Tunnel | — | — | pcastagentd (such as for control operations and camera) |

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| 8443 | TCP | iCal service (SSL) | — | pcsync-https | Mac OS X Server v10.5 or later (JBOSS HTTPS in Mac OS X Server 10.4 or earlier) |
| 8800 | TCP | Address Book service | — | sunwebadmin | Mac OS X Server v10.6 or later |
| 8843 | TCP | Address Book service (SSL) | — | — | Mac OS X Server v10.6 or later |
| 8821, 8826 | TCP | Stored | — | — | Final Cut Server |
| 8891 | TCP | ldsd | — | — | Final Cut Server (data transfers) |
| 9006 | TCP | Tomcat standalone | — | — | Mac OS X Server v10.6 or earlier |
| 9100 | TCP | Printing | — | — | Printing to certain network printers |
| 9418 | TCP/UDP | git pack transfer | — | git | Xcode Server (remote git) |
| 10548 | TCP | Apple Document Sharing Service | — | serverdocs | macOS Server iOS file sharing |
| 11211 | — | memcached (unregistered use) | — | — | Calendar Server |
| 16080 | TCP | — | — | — | Web service with performance cache |
| 16384–16403 | UDP | Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP) | — | connected, — | Messages (Audio RTP, RTCP; Video RTP, RTCP) |
| 16384–16387 | UDP | Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP) | — | connected, — | FaceTime, Game Center |
| 16393–16402 | UDP | Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP) | — | — | FaceTime, Game Center |
| 16403–16472 | UDP | Real-Time Transport Protocol (RTP), Real- | — | — | Game Center |

| Port | TCP or UDP | Service or protocol name | RFC | Service name | Used by |
|---|---|---|---|---|---|
| | | Time Control Protocol (RTCP) | | | |
| 24000–24999 | TCP | — | — | med-ltp | Web service with performance cache |
| 42000–42999 | TCP | — | — | — | iTunes Radio streams |
| 49152–65535 | TCP | Xsan | — | — | Xsan Filesystem Access |
| 49152–65535 | UDP | — | — | — | Back to My Mac |
| 50003 | — | FileMaker server service | — | — | — |
| 50006 | — | FileMaker helper service | — | — | — |

# 12.