# Deployment and Network Requirements

### Network Requirements

Each one of the MVISION Cloud servers should have at least one IP that should be accessible to the other servers. An  MVISION Cloud system usually requires a public IP address so it can be accessed from anywhere on the internet when inbound traffic such as email, Salesforce callouts, remote users, etc. is involved.

The HTTP/HTTPS and SMTP traffic that is designated to the public IP address should be routed to the Encryption Proxy. When two or more proxies are used, the traffic should be routed through a Network Load Balancer (NLB). In addition, a Token Dictionary (an external dictionary database) must be accessible from the encryption proxies.

The following tables indicate the required ports, protocols and source IP for each server.

#### MVISION Cloud Secure Gateways

| Port | Protocol | Inbound | Outbound | Notes |
| --- | --- | --- | --- | --- |
| 25 | TCP | Salesforce MX | Any | For SMTP (Qmail), when email-to-case, chatter replies, SFO etc. are used, the Outbound can also be Salesforce end-user |
| 80 | TCP | Salesforce end user | Salesforce.com | HTTP |
| 443 | TCP | Salesforce end user | Salesforce.com | HTTPS |
| 443 | TCP |  | MVISION Cloud Cloud | HTTPS for Policy/Config updated and audit events. |
| 1521 | TCP |  | Token Dictionary Database | Use this port when Oracle is configured as the database (Oracle Net Listener). **NOTE:** This is the default port, but it may be different depending on your database server config. |
| 2049 | TCP and UDP |  | File Server | When using NFS protocol for file residency (NFSv4/rpc) |
| 3306 | TCP |  | Token Dictionary Database | Use this port when MySql is used as the database.  **NOTE:** This is the default port, but it may be different depending on your database server config. |
| 5696 | TCP |  | Key Server | KMIP TTLV over SSL. |

#### MVISION Cloud

| Port | Protocol | Inbound | Outbound | Notes |
| --- | --- | --- | --- | --- |
| 443 | TCP | MVISION Cloud Secure Gateways |  | HTTPS for policy/config updates and audit events. |

#### Token Dictionary

| Port | Protocol | Inbound | Outbound | Notes |
| --- | --- | --- | --- | --- |
| 1521 | TCP | MVISION Cloud Secure Gateways |  | Use this port when Oracle is configured as the database (Oracle Net Listener). **NOTE:** This is the default port, but it may be different depending on your database server config. |
| 3306 | TCP | MVISION Cloud Secure Gateways |  | Use this port when MySql is used as the database.  **NOTE:** This is the default port, but it may be different depending on your database server config. |

#### File Server

| Port | Protocol | Inbound | Outbound | Notes |
| --- | --- | --- | --- | --- |
| 2049 | TCP and UDP | MVISION Cloud Secure Gateways |  | NFS port |

### Reverse Proxy Requirements

The following settings are required to enable the reverse proxy functionality within MVISION Cloud, and in order for MVISION Cloud to intercept the traffic between the organization’s users and Salesforce.com.

**Domain Names.** A unique list of domain names should be assigned to the MVISION Cloud secure system. These domains, when resolved, should direct to the MVISION Cloud Secure public IP.

**SSL Wildcard Certificate.** A valid SSL wild card server certificate should be provided. This certificate secures the selected MVISION Cloud Secure’s domain name and its subdomains (the domain names that were selected by the organization for the reverse proxy functionality).

**A Records.** DNS “A record” should be defined either for the MVISION Cloud wildcard domain or for each MVISION Cloud domain name. In the case of the wildcard domain or specific domain name(s), the DNS entry should point to the public IP address of the MVISION Cloud Secure Gateway.

**MX Records.** MVISION Cloud is involved in encrypting emails that are being transferred through Salesforce in some deployments. In order for this to happen, an MX record should be defined to route these emails through MVISION Cloud.

During the encryption process, the original recipient email address is changed to another email address under the mx record defined in the MVISION Cloud secure system. During the decryption process, the MVISION Cloud Secure system changes the recipient email address back to the original address.

### File Residency Requirements

If the File Residency functionality is required in your environment, a file server accessible to the MVISION Cloud secure system via the NFS protocol is required. Additionally, the File Tokenization option should be selected in the policy.

The File server should be accessible from the MVISION Cloud Security Gateway(s) and should have a designated shared directory. The shared directory needs to have full permissions (read, write, and execute) for users, groups, etc.

The following steps are given as an example to preparing the File server that has a Linux operating system installed and using the /var/nfs directory as the designated shared directory:

1. On the file server, run the following command:

vi /etc/exports

1. Add the following row:

/var/nfs \*(rw,no\_root\_squash)

1. Run the following commands:

mkdir /var/nfs

chmod 777 /var/nfs

/sbin/service portmap start

service nfs start

### High Availability

For high availability environments, you can use multiple Encryption Proxy servers that run behind a load balancer that supports SMTP, HTTP, and HTTPS protocols. The load balancer configuration is determined in accordance with the manufacturer and model your organization is using. Consult the load balancer’s documentation for the specific configuration details.

General MVISION Cloud Secure requirements during the load balancer configuration are:

Open ports 25, 80 and 443.

• Set an HTTP health check where:

• The send string is set to:

GET /servlet/Version?lb=loadBalancerToken HTTP/1.1\r\nHost:\ <customer org><customer Skyhigh Secure domain>.com\r\n\r\n

• The HTTP return status code is set to 200 OK