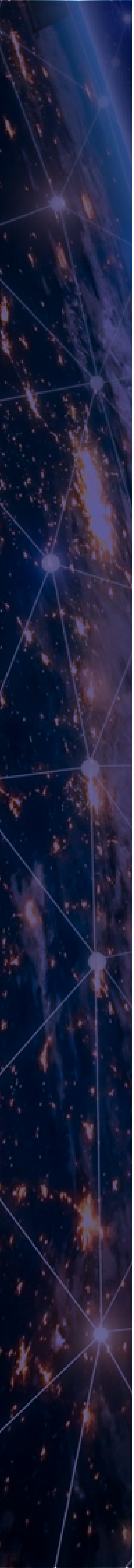


Iris Networks Cloud & Security managed services MA3-4, Service Description

1.0 Definitions

Alert: A log received from the Device/Asset, parsed by VisionLink, and sent to ProVision
Client or Customer: The company procuring the managed service
Co-Management: The Client and Foresite have full access to the Device/Asset for any changes or updates
Device/Asset: A combination of hardware, software and licensing that is to be monitored/managed as part of the Service
Event: An activity that has been identified by ProVision to represent a potential threat that warrants additional triage by the SOC analysts to determine the nature of the activity
Incident: An activity positively identified as a breach in progress and warrants immediate engagement of Client incident handling and response personnel
Log: A record of activity written by a security device, network element, computing platform, etc. for such purposes as recording events, errors, status messages, or other operating details
OBQ: OnBoarding Questionnaire. A document or online tool to gather all the required information to set up the Service.
OnBoarding: The activities and process to bring the Client in to live Service.
POC: Client point of contact for managed service
ProVision/Portal: Iris Networks Cloud & Security next-generation cloud-based managed services platform
Service Level: Monitored, Managed or Co-Managed
SOC: Global security operation centers with primary SOC located in Overland Park, KS, and supporting operations centers located in East Hartford, CT and London.
SOW: Statement of Work
Ticket: Comes in various forms such as, but not limited to;
• Support Ticket – Used to log and progress Tickets of a support nature (e.g. creation of a new user)
• Security Incident Ticket - An activity positively identified for further investigation that warrants follow up (e.g. Suspected Security Issue)
• Change Request Ticket – Used for creating requests for workload to be implemented (e.g. updating a set of Rules).
VisionLink: Foresite Client premise appliance responsible for log and security stream aggregation and processing as part of the cloud-based ProVision managed services platform.

2.0 Solution Overview

Iris Networks Cloud & Security managed services have two levels supporting Co-Managed & Fully Managed options as outlined in the table below;

Managed Service	MA3 Co-managed	MA4 Fully Managed
Security Information Event Monitoring	✓	✓
ProVision Web Customer Portal	✓	✓
Reporting	✓	✓
Alerting	✓	✓
Notification & Escalation	✓	✓
24x7x365 Analysis	✓	✓
Full r/w access to infrastructure	✕	✓
Incident Remediation	✓	✓
Change Requests	✓	✓
System Upgrades*	✓	✓
System Configuration Backup**	option	option

*System Upgrades are included for minor upgrades that can be performed remotely. If onsite work is recommended and required, this will be covered by an additional SOW.
**Backups of the Device/Asset are the responsibility of the Client. At Client request, our team will perform a manual configuration backup prior to implementing any Change Requests, subject to the technology allowing it.

3.0 Service Scope

Hours of Operation: Iris Networks Cloud & Security managed services are delivered through Foresite Security Operations Centers (SOCs) which operate 24 hours per day, 7 days per week, and 365/6 days per year.
Language Support: All Services, Portal and communications are provided in English language only.
Monitoring: Iris Networks Cloud & Security will monitor and analyse the log stream from the Device/Asset under Service. The log source will vary dependent on technology but is typically syslog. Monitoring will be conducted 24/7/365. Client shall make available log feeds for monitored devices, which will be sent to Foresite on premise collector, Visionlink
Management: In addition to the monitoring, Iris Networks Cloud & Security will provide management services for the Device/Asset that include policy updates, rulebase changes and any configuration changes as required for the operation of the service.

• **Fully Managed (MA4)** means that the Client will only have read-only access to the Device/Asset and Foresite will have full ownership for effecting any changes. Client requested changes should be logged in the ProVision Portal using a Change Request Ticket.

• **Co-Managed (MA3)** means that the Client can have the same full access to the Device/Asset as Foresite to perform any changes as appropriate. If the Client does make any changes to the Device/Asset, it should be logged within the ProVision Portal using a Change Request Ticket to keep track of all updates. Client can use a combination of Client implemented and Foresite implemented changes throughout the lifetime of the Service.

All Iris Networks Cloud & Security activities will be implemented remotely. In the event of issues that require physical or local access to the Device/Asset, Client may at times be required for assistance to trouble shoot (e.g. system rebuild, power-cycle, reboot or console access).

Alerting & Escalation: Log streams collected by VisionLink are parsed, normalised, and sent to the ProVision threat engine for additional analysis. The business rules in the threat engine raise any suspicious logs or patterns of behavior to an Event. Event conditions that are deemed of interest or worthy of follow up will be brought to the attention of the Client's designated POC(s) by the creation of a Ticket within ProVision. Events are classified in to 4 severities;

- **Emergency** – Existence of conditions which indicate a potential security incident has occurred
- **Critical** – Existence of conditions which indicate the presence of a potential security threat requiring attention
- **Warning** – Potential Incidents that may have been averted but warrant investigation and confirmation
- **Informational** – System and vendor information to bring additional context to higher priority Events

All progress of Incidents will be tracked within the ProVision Ticket. The SOC may also call the Client depending on the severity of the Incident. Communication preferences are confirmed during OnBoarding and can be adapted throughout the lifetime of the Service.

Ticketing: Ticket types include but are not limited to the following; Security Incident, Support Ticket and Change Request. The assignee of a Ticket will always be a Foresite SOC representative and if the status of the Ticket is set to "Waiting for Customer', then the progress of the Ticket is the responsibility of the Client's designated POC(s). Tickets have 4 severity levels as below;

- **P1 Emergency** – System down or potential security Incident that warrants urgent attention
- **P2 Critical** – Significant impact that could lead in to a security Incident or system outage if not addressed
- **P3 Warning** – Moderate loss of functionality or security that should be addressed
- **P4 Informational** – Supporting information and notification of behavior

The SOC Analyst will work closely with the Client's designated POC(s) to progress and resolve the Ticket where appropriate. If the Client doesn't respond to the Ticket in a timely manner, Iris Networks Cloud & Security reserves the right to close the Ticket and tune out the logs to stop it reoccurring.

Tickets can be updated/progressed within the ProVision Portal or via email by responding to the Ticket update email that will get sent to all those set as a 'Follower' within the Ticket. 'Followers' can be automatically assigned for all Client Tickets or individually depending on the actual Ticket. 'Followers' are confirmed during OnBoarding and can be adapted throughout the lifetime of the Service.

Log Retention: Foresite stores ProVision security stream data consisting of processed log information (Alerts) for a period of 90 days, unless otherwise specified in the SID (Service Initiation Document). Aggregated data used for the Reporting is available throughout the lifetime of the Service. Further log retention services are available as an additional service offering.

Additional Checks: Iris Networks Cloud & Security can apply additional checks to a Device/Asset depending on requirement. These checks include ICMP (Ping), HTTP, HTTPS, & SSH. Any additional checks are confirmed during OnBoarding and can be adapted throughout the lifetime of the Service.

4.0 ProVision Portal

Iris Networks Cloud & Security provides the ProVision Portal for access to the Service. The Portal is the interaction between the SOC Analysts and the Client. Through the ProVision Portal, Clients can;

- View Dashboards for summary of Service
- Manage Devices/Assets and system inventory
- View and search Alert logs and Events
- View and update profile information
- View and update Client information
- Access Reports
- Search, update and manage all types of Tickets
- Access appropriate Knowledge Base articles

5.0 Reporting

Iris Networks Cloud & Security provides a multitude of preconfigured reports that are all available in the ProVision Portal. Reporting is very flexible, including custom and quick date ranges, Device/Asset or Account information, tabular or graphical view in a variety of different formats including bar graphs, line graphs, heat maps and more. Reporting includes but is not limited;

- Monthly Management Report (Overview of Service for the monthly period)
- Estate (Users, Managed Assets/Devices)
- Tickets (Management Report, Support Tickets, Security Tickets, Change Requests)
- Authentication (Management Report, Summary Report, By User, By Device, By Disabled Accounts)
- Accounts (Created, Disabled, Deleted, Enabled, Locked, Password Activity)
- Security Analysis (Management Report, Events, Log Messages, Anti-Virus, Policy Changes)
- Traffic (Management Report, Dropped Traffic, By Source, By Destination, By Destination Port)

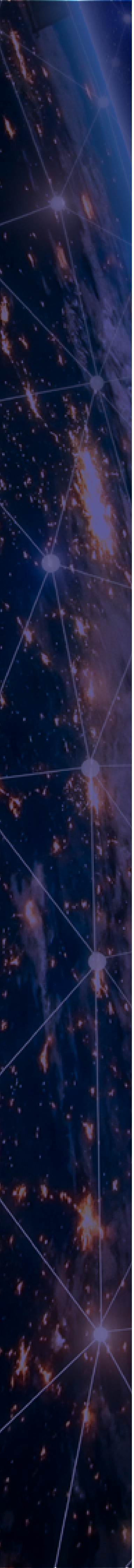
Additional Reports can be requested during OnBoarding and can be adapted throughout the life-time of the Service (subject to availability of data). With the aim of continuous improvement, Iris Networks Could & Security reserves the right to add/remove/change the reporting in the ProVision Portal.

6.0 VisionLink

Iris Networks Cloud & Security managed services require VisionLink, which works as the log collector. VisionLink is typically located on the Client site and receives the log stream of the Device/Assets associated with the Service. VisionLink comes in 2 formats;

- Hardware appliance
- Software / Agent that is installed on to a Client provided VM infrastructure

VisionLink Appliance: This will be hardware supplied by Iris Networks Cloud & Security to be installed at the Clients site. Connectivity must be provided according to the VisionLink Installation Guide and is set up during OnBoarding. If the hardware appliance should fail and require RMA, it is the Clients responsibility to package and return it to Iris Networks Cloud & Security. Iris Networks Cloud & Security will supply replacement hardware.



VisionLink VM: Iris Networks Cloud & Security will either provide the image for the VisionLink to the Client for installation or Client will provide the resources in a VM for Iris Networks Cloud & Security to install the VisionLink Agent. Specifications for the VM will depend on the number of Devices/Assets in the Service and will be worked out during OnBoarding but is typically Quad-core, 1TB HDD and 4GB Memory. The VisionLink agent is installed on Ubuntu 16.04 LTS (or later approved system). It is the Clients responsibility to ensure that the VM is available for the Service.

7.0 OnBoarding

Iris Networks Cloud & Security will work with the client to bring all Devices/Assets in to live Service during the OnBoarding process. This is typically 30-60 days but will depend on the size of the estate and commitment of resources.

The OnBoarding consists of 2 parallel streams;

- **Technical** – to set up the infrastructure required for the service. This includes; Installation of VisionLink, collection of logs, creation of Events & Tickets, Portal training.
- **Information Gathering** – to provide as much context as possible to enrich the analysis. This involves either completing a document or online tool to gather all the required information to set up the Service. Areas covered are contact details, facilities, network design, topology, platforms, apps and users.

Once the OnBoarding is complete, the Service is considered live. All this is handled and communicated through

8.0 Service Level Agreement (SLA)

There are 3 targets measured for the SLA as follows;

- **Availability of the ProVision Portal**
- **Events** - Time to respond and target to address
- **Tickets** - Time to respond and target to address (Support & Security Incident Tickets)

'Time to Respond' is measured from when the Event or Ticket is created to when it is first touched by a SOC Engineer.

'Target to Address' is the target time for the analysis of an Event.

'Target to Resolve' is the target time to implement a workaround or fix for the Ticket.

Availability of the ProVision Portal: Foresite ProVision Portal is guaranteed available 99% of the time over a one-year period and measured annually.

Events:

Priority	Time to Respond	Target to Address
Emergency	15 Mins	1 hour
Critical	30 mins	2 hours
Warning	2 hours	8 hours
Informational	n/a	n/a

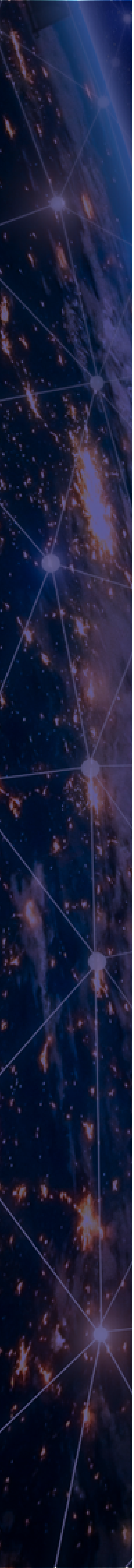
Tickets:

Priority	Time to Respond	Target to Resolve
P1 Critical Impact	1 hour	TTR + 4 hours
P2 Significant Impact	4 hours	TTR + 8 Hours
P3 Normal/Minor	24 hours	72 hours
P4 Low/ Information	48 hours	7 days

SLA Exceptions: The following exclusions are not included in the SLA calculation:

- Scheduled maintenance work required by Foresite
- Change management requirements affecting managed devices
- Circumstances beyond the reasonable control of Foresite
- Changes to a managed device not performed by Foresite
- Loss of connectivity due to Client connectivity issues or Client managed issues

SLA Failure Rebate: At Client's request, Iris Networks Cloud & Security will pay a rebate each year (following each 12 months of service) in the format of a service credit which can be used to purchase additional services or extend the service period if the SLA has not been met. Customer must log the request for a rebate as a Ticket in the ProVision Portal within 30 days of the proposed missed SLA. Total service credit Rebates cannot exceed 10% the total annual service charge.



Measure	Credit
Availability of the ProVision Portal	Half a day service credit for every whole hour the SLA is missed
Events (Response)	1 hour service credit for every Event that misses the Response SLA
Tickets (Response)	1 hour service credit for every Ticket that misses the Response SLA

Maintenance Window: With the unique ProVision infrastructure, it is very rare that Maintenance Windows are required that incur an interruption to the Portal or Service. Should there be a requirement for a period of time to conduct any maintenance, Iris Networks Cloud & Security reserves the right to communicate that Maintenance Window in advance through the notification system in the Portal.

9.0 Client Pre-requisites 9.0 Client Pre-requisites

The following requirements must be confirmed by the Client for the operation of the Service;
- **Device/Asset** – suitable infrastructure to be included in the Service
- **Software License/Subscriptions** – any Device/Asset in the Service must have the appropriate full manufacturer's product license and subscriptions for the duration of the Service. Device/Assets of Software that are considered end of life by the manufacturer are not covered by the Service
- **Hardware Support** – All Devices/Assets must have the appropriate full manufacturer's support for the duration of the Service
- **Software limitations** - only the manufacturer's application(s) and operating system are to be run on the Asset/Device
- **Security Operation** – All Devices/Assets that are brought in to the Service must contain a valid rulebase or configuration to protect the security of the Service. Foresite reserves the right to audit any such configurations and remedial work may be required to address any issues
- **Connectivity** - Client will ensure client-side access and connectivity to all Device/Assets as appropriate. Foresite is not responsible for resolving Client's Internet Service Provider (ISP) outages, or issues with Client's internal network or computing platform infrastructure
- **Log Stream** – typically syslog or snmp but dependent on Vendor. It is the responsibility of the client to ensure the log stream is directed at VisionLink for Service operation.
- **Client Point of Contact (POC)** – The Client is responsible for providing Iris Networks Cloud & Security a primary point of contact (POC). The POC will provide access to knowledgeable technical staff, and/or third-party resources, to assist Foresite with any hands-on support or working with third-party vendors

10.0 Exclusions

The following (without limitation) are not included in the Service;
- **Site Visits (on-site Support)** - Any site visits by Iris Networks Cloud & Security are not included with the Service. Any required visits can be negotiated under a Iris Networks Cloud & Security professional services agreement
- **Services for Device/Assets not covered within the Service**
- **Remedial work** – Any issues caused by Client initiated Changes or failed Changes are not covered by the Service. Foresite operate a Fair Use Policy for the number of Tickets and Change Requests used in the Service. There is no limit on the number of Security Incident and Support Tickets used but Foresite reserve the right to review the volume of Change Requests per Client if it is determined that the Change Requests are being improperly used.

11.0 End of Agreement (close-down)

The following (without limitation) closed-down activities apply at the end of the Service period;
- Iris Networks Cloud & Security will close the ProVision Client account and all User accounts for the ProVision Portal
- All copies of VisionLink must be wiped clean and deleted by the Client. If VisionLink resides within a Client VM, it is the Clients responsibility to delete it and confirm when it has been completed to Iris Networks Cloud & Security. If VisionLink is supplied as hardware, Client retains the hardware. For clarification, it does not need to be shipped back to Iris Networks Cloud & Security
- Iris Networks Cloud & Security will delete all logs and data stored within ProVision 30 days after the end of the Service period. If the Client choses to retain the data, Client must provide suitable storage for the logs to be shipped to. END.