clearswift
by HelpSystems

Customer Support Handbook

May 2019

Contents

HelpSystems, LLC. All trademarks and registered trademarks are the property of their respective owners.

Glossary

Category	The incident category as described in the Service Description.
Defect	An error/malfunction that causes the Clearswift software to function outside of material conformity with the software documentation.
Enhancement Request	Any request to change the functionality, performance or scope of the software/solution that is not directly related to a defect.
Gateway	The hardware and any pre-installed Clearswift products.
Hardware	The server supplied as part of the Gateway.
Incident	Any event which is not part of the standard operation of the Clearswift product or solution which causes, or may cause, an interruption or a reduction in quality.
Incident Severity	The categorisation of a reported Incident based on impact and prioritisation as defined within the terms of the Service Description.
Problem Report	Engineering case defining a state, identified from Incidents, that indicates a defect in the product or solution.
SCR	Software Change Request defined within a Problem Report to resolve a defect or deliver against an Enhancement Request.
Service Description	The document defining the level of service to be provided by Clearswift Support.
Service Desk	The Clearswift Support team responsible for delivery of services as described in the Service Description.
Service Hours	Help desk support during Clearswift Support centre hours.
Service Level Targets	Stated commitments for the delivery of support services as detailed in the Service Description.
Support Portal	The channel provided to enable customers to raise Incidents with Clearswift Support via a web based tool.
Support Services	The support and maintenance services performed by Clearswift pursuant to the Service Description.
Technical Contact	A customer registered in the support incident management system authorised to raise incidents via the support portal and receive support.

Section 01: Introduction

Clearswift is dedicated to optimising the success of our customers and to attaining the highest levels of customer satisfaction through the delivery of professional, efficient and high quality support across the Clearswift product portfolio.

Clearswift delivers support to its customers under the terms of a Support Agreement, offering tiered service levels designed to provide flexibility in meeting a variety of customer business needs.

1.1 Purpose

The purpose of this document is to describe the support offerings available from Clearswift and how the services defined within those offerings are delivered to our customers. This document is designed to be viewed both as a stand-alone reference and as an addendum to the Clearswift Support Agreement.

1.2 Scope

This document applies to Clearswift proprietary software product(s) and solutions licensed to the customer under the Clearswift License Agreement and covered under the terms of the Clearswift Support Agreement. All references to Clearswift product in this document refer to such licensed product. Please refer to the Clearswift Support Agreement for details on maintenance terms and conditions.

Note: This document will be revised periodically to reflect changes in the products and solutions being supported and the processes, procedures and technologies being used to deliver support services. The latest version of this document is posted on the Clearswift Support Portal (www.clearswift.com/support/ portals).

1.3 Referenced documents

- Clearswift License Agreement
- Clearswift Support Agreement
- Clearswift Service Description

Section 02: Support Services

Clearswift recognises that good support is fundamental to extracting the full benefit from Clearswift solutions. We aim to maximise our customers' investment through the delivery of comprehensive service offerings. Our services are developed to cater for the different needs of our customers and to ensure ongoing and consistent operational capabilities throughout the lifetime of the solutions.

2.1 Tiered Support Offerings

Clearswift provides three tiers of support:

- **Standard -** a highly reactive and responsive 24x7 service, enabling Clearswift to take immediate ownership of reported issues, providing full visibility of progress and status through the end-to-end management of incidents. Customers automatically receive standard support as part of their solution.
- **Standard Plus -** designed for clients with fewer than 2,000 users who want to take advantage of the proactive alerting functionality built into the Clearswift solutions. This functionality offers faster problem resolution by automatically creating new support cases with Clearswift when certain key alarms are raised.
- **Advanced -** delivers enhanced support capabilities including automated service monitoring, reporting and regular service reviews, to further secure consistent operational availability through a more proactive level of support.
- **Premium -** a highly intimate service delivering additional value add services through a Support Account Manager (SAM), inclusive of best practice consultation, an annual service health check, on-site support days and regular on premise service reviews.

2.2 Global Presence

Clearswift delivers support through service desks located in Europe, the US and APAC regions. We provide 24x7 access to support via a follow-the-sun service model, alongside a web based support system and knowledge base that facilitate continuous support and self-help.

2.3 Clearswift Support Portal

Access to support is provided via a dedicated online portal at **www.clearswift.com/support/portals**. The Support Portal provides a personalised interface to Clearswift support and many other useful resources. Technical Contacts can use the Support Portal to report new Incidents, submit requested information and to monitor service progress, with automatic emails providing notification of updates.

Section 02: Support Services

2.4 Evolutionary Upgrade Releases

Our customers' investment in our solutions drives their information security strategy today and into the future. Our support offerings are designed to ensure the future success of that investment through ongoing entitlement to new, innovative and visionary releases of the licensed products, as they evolve:

- **Version releases (X.y.z)** – delivering significant core change in the software scope (such as adding new functionality or a change in the software architecture).
- **Major releases (x.Y.z)** – delivering modifications to existing functionality or additional functionality in existing software modules.

Version and major releases future-proof strategic investment by providing certification against higher releases of embedded third party components and porting to the latest platform vendor technologies. These releases may also leverage new technology architectures, provide cross-product integration capabilities and introduce new functionality and efficiencies to reduce the Total Cost of Ownership (TCO) of Clearswift solutions.

2.5 Maintenance Releases

Clearswift's commitment to consistent product quality and performance is backed by measures to proactively adjust and update core products in line with market developments and technology advances, while reactively releasing periodic service packs to continuously improve the underlying operation of products and to resolve and prevent problems.

Through the product maintenance cycle, Clearswift provides:

- **Patch releases (x.y.Z)** – delivering multiple Software Change Requests (SCRs) to correct and resolve Defect Problem Reports and deliver against Enhancement Requests.
- **Hot fixes** – emergency, temporary patches correcting a single, component-level SCR to resolve a critical Defect Problem Report.

All customers with active support agreements are entitled to receive upgrade and maintenance releases for their Clearswift products under license.

2.6 End of Life (EOL) Policy

The nature of the support provided by Clearswift for any given licensed product will depend upon where a product release is within the product life cycle. While Clearswift provide for reasonable longevity in the support of all releases, we also deliver sufficient change in our products aligned to ongoing market trends and technology requirements and End of Life (EOL) older releases as required.

Clearswift encourages customers to keep up to date with releases to ensure that they are achieving the maximum benefit from their deployed solutions and are eligible for support. Under the terms of our product EOL policy, Clearswift treat both version and major releases as a new upgrade release and commit to providing support and maintenance services for the latest (n) and previous (n-1) upgrade release. The product life cycle stages are defined below.

2.6.1 Full Support (prior to EOL)

This defines the standard term of support for the current release (n), with customers eligible to receive technical support, services and maintenance updates for products under license.

2.6.2 Sustaining Support (prior to product EOL)

This defines the standard term of support for the product version previous to the current release (n-1) and is available until the stated EOL date for that release. During this period, customers will not receive ongoing patch releases, but hot fixes may be made available to resolve critical Defect Problem Reports.

2.6.3 Extended Support (beyond product EOL)

This defines the standard term of support for releases that reach EOL (n-2). This is a support-only term provided for one year beyond stated EOL. During this period, customers are not eligible to receive further maintenance releases as the code branches for EOL releases are closed. Extensions to this period of support are negotiable, with a potential uplift in the price of the Support Agreement to cover any additional cost incurred by Clearswift in delivering ongoing services.

2.6.4 End of Support Life (EOSL)

Any release that is not subject to the terms of an Extended Support Agreement will move into End of Support Life (EOSL). At this point, Clearswift will stop providing any level of support for the product, other than self service support provided by our online knowledge base and associated documentation pertaining to the release. Where customers do request support for EOSL product, Clearswift will use reasonable efforts to provide support on a one-time basis, providing the necessary information to assist customers in upgrading to the latest supported version.

Section 03: Support Offerings

Clearswift provides tiered support offerings in order to meet your specific needs. All offerings are built from an essential foundation support tier which can be further enhanced with additional services.

3.1 Support at a Glance

Description	Standard	Standard Plus	Advanced	Premium
Support access via phone, web portal and email	✓	✓	✓	✓
24x7 support (excluding 6 stated public holidays)	✓	✓	✓	✓
24x7 access to the Clearswift Support Portal knowledge base	✓	✓	✓	✓
2 registered technical contacts per licensed instance	✓	✓	✓	✓
Access to new version upgrade releases	✓	✓	✓	✓
Automated maintenance release updates	✓	✓	✓	✓
Defined service level targets for incident response and resolution	✓	✓	✓	✓
Proactive communications (forums and RSS service feeds)	✓	✓	✓	✓
Proactive system monitoring and exception reporting	×	✓	✓	✓
Named contact for fast-track escalation and service reporting	×	×	✓	✓
Annual system health check	×	×	✓	✓
Quarterly service reviews (telephone)	×	×	✓	✓
1 additional technical contact per licensed instance	×	×	✓	✓
Assigned Support Account Manager (SAM)	×	×	×	✓
2 dedicated support days (on-site)	×	×	×	✓
Quarterly service history reviews (on-site)	×	×	×	✓
Best practice policy, modifications and compliance recommendations	×	×	×	✓
Bespoke roadmap and release briefings	×	×	×	✓
Dedicated support infrastructure replicating your content security policy	×	×	×	✓
Documented critical incident reports	×	×	×	✓

3.2 Standard Support

Every supported customer is entitled to our standard 24x7 support offering, delivered via telephone, email and our web portal. This highly reactive and responsive service allows us to take immediate ownership of any reported issues, providing you with full visibility of progress and status throughout the lifecycle of the incident. Our highly trained and experienced technical support engineers are located strategically around the world and offer response times as rapid as just one elapsed hour.

Along with the expected product updates, your support includes subscriptions to live service feeds that will keep your organisation protected from the latest threats. Depending on the product, these include antivirus, anti-spyware, anti-spam updates and the latest filter information from Clearswift's world-leading URL database.

You'll be entitled to two registered technical contacts per licensed instance of your Clearswift solutions. These contacts can raise support incidents with our support engineers and they'll also benefit from full access to our extensive, searchable knowledge base. This valuable and detailed resource gives you access to hundreds of solutions, information on hot topics and recommendations on best practice.

You can also contribute to the product roadmap by raising product enhancement requests.

Our standard offering includes:

- 24x7 service desk support, with weekend calls routed to on call engineers via a call logging service
- 24x7 access to the Clearswift support portal for access to our knowledge base and extensive self-help resources
- First line (L1) application/product support for initial review and response to customer service requests and escalation of unresolved issues to technical support specialists
- Second line (L2) technical support through product specialists and subject matter experts for the provision of comprehensive diagnostic and root cause analysis and Incident resolution
- Third line (L3) escalation support through product development engineers for the provision of Problem
- Subscriptions to live service feeds providing protection from the latest threats, including anti-virus and spyware updates and the latest filter information from Clearswift's world-leading URL database
- Entitlement to future, evolutionary upgrade releases for licensed products
- 2 registered technical contacts per licensed instance of your Clearswift solution(s)

3.3 Standard Support

The standard plus support offering is designed for clients with fewer than 2,000 users who want to take advantage of the proactive alerting functionality built into the Clearswift solutions.

This functionality offers you faster problem resolution by automatically submitting alarms back to the Clearswift incident management system to create new cases. These cases will be automatically assigned to a support engineer and they'll contact you to resolve the issue, with a targeted response time of 30 minutes during normal working hours.

HelpSystems, LLC. All trademarks and registered trademarks are the property of their respective owners.

Section 03: Support Offerings

3.4 Advanced Support

Our advanced support offering is ideal for customers that require a more proactive level of service. In addition to the many benefits included in our standard support offering, you'll benefit from:

- A single point of contact for fast-track escalation, ensuring that critical issues are resolved promptly and to your satisfaction
- Proactive system monitoring and exception reporting
- Quarterly remote reviews of your service history and usage trends to identify where additional resources may be necessary
- Briefings on forthcoming releases and how you can best implement new functionality
- An additional technical contact per licensed instance of your Clearswift solution(s)

Our proactive system monitoring service makes use of the call home functionality of our products to allow us to remotely monitor key performance metrics on your system. In the event that an alarm is raised, we'll contact you in order to resolve the issue.

Key alarms will automatically generate high priority support incidents that we aim to respond to within 30 minutes. Less critical alarms will also automatically generate support incidents and these will be dealt with according to our standard response timeframes. To view the status assigned to each Gateway alarm, please refer to:

- Appendix A - Web Gateway Alarm Severity
- Appendix B - Email Gateway Alarm Severity

Our ability to remotely monitor key performance metrics on your system allows us to provide our advanced and premium support customers with quarterly trend reports. These reports allow you to measure performance and usage over time so that you can predict when you might need to add additional resources to cope with increasing Internet or email throughput. The quarterly trend reports will provide you with information on such things as:

- Mail flow
- Internet traffic
- Hard disk usage
- Database size

3.5 Premium Support

Premium support customers receive unmatched levels of assistance. Our premium service builds on the standard and advanced offerings, providing you with a personalised, high value service through a Support Account Manager (SAM). While issue reporting and resolution continue to leverage the existing channels, your SAM is available for fast-track escalation and will engage with you regularly through:

Our standard offering includes:

- An annual health check, evaluating your current operations and providing you with recommendations for improvement
- Two on-site support days for problem resolution, system evaluation and knowledge transfer
- Quarterly service history reviews and documented critical incident reports
- Discussions on best practice and compliance requirements
- Briefings on forthcoming releases
- Updates on status of software change requests (SCRs)
- Bespoke roadmap briefings

We'll also maintain a dedicated support environment that replicates your current content security policy, which will help to ensure faster resolution of any support incidents.

HelpSystems, LLC. All trademarks and registered trademarks are the property of their respective owners.

Section 04: How to Engage Clearswift Support

The Clearswift Support services are designed to offer a seamless incident handling experience so that customers always know the status of their open incidents. The support process is based on a well-defined, transparent case flow methodology. From initiation through to resolution, this methodology ensures that Clearswift takes ownership of incidents and efficiently advances them across the different levels of the support organisation.

4.1 Technical Contacts

Only registered Technical Contacts are permitted to open or update incidents. Technical Contacts should be suitably trained on Clearswift software products prior to opening any incidents.

4.2 Support Communication Channels

Clearswift offer various communication channels for support. The Clearswift Support Portal is the most efficient and preferred channel for raising incidents and providing updates, but service requests can also be initiated by telephone and email. The following channels are available:

Channel	Service	Description
Support Portal	www.clearswift.com/support/portals	The most efficient method for creating incidents and finding updates.
Telephone	APAC: +61 2 9424 1210 EUROPE: +44 (0)118 9038200 GERMANY: 0800 1800 556 JAPAN: 0066 33 812 501 US: +1 856 359 2170	The recommended communication method for critical/high severity issues that require rapid response and action.
Email	support@clearswift.com	For users who experience difficulties using the Support Portal, email is a suitable alternative.

This information may be updated periodically and can be verified at the following web page:
www.clearswift.com/support

Section 05: Incident Management

To maintain effective communications with our customers, the handling of incidents flows through an agreed chain of actions.

When issues are identified, the Technical Contact will carry out an impact analysis and raise the incident with the Clearswift support team providing the following information:

- Product and version
- Incident description/symptoms
- Supporting information (log files, configuration files, etc.)
- Contact details where required
- Impact and urgency

Each incident has a unique ID number. Clearswift Support will allocate an Incident Category and Severity which will be acknowledged via email.

Note: Before a customer can create an incident, they must be registered with Clearswift as a Technical Contact. To register, please contact Clearswift Support or log on to: **support.clearswift.com**

5.1 Incident Category

The first step in the support process is to determine the nature of the support requirement. There are four categories of incident available to customers via the Clearswift Support Portal.

Incident Category	Description
Technical Query	A query relating to specific software or system use/functionality, or general enquiry related to Clearswift products.
Problem Report	An error in the use/function of the software.
Enhancement Request	A request to modify the product to overcome known limitations or functional gaps.
Hardware Incident	An error in the use/function of the hardware.
Proactive Alert	A system generated notification based upon breach of configured parameter thresholds. *Reserved for Advanced and Premium Support customers.

Section 05: Incident Management

5.2 Incident Severity

The responsiveness of Clearswift Support is driven by the severity of an incident. Incidents are assigned a severity level by support, but this may be changed after consultation with the Technical Contact, if it is reasonable to do so in accordance with the severity levels as defined below.

Severity	Description
1 Critical	System functionality is completely unavailable or inaccessible. The situation requires immediate attention. Example scenarios: • All services unavailable on a single platform - total loss of service • Services unavailable to a multitude of platforms • Suspected security breach
2 High	System functionality is severely limited, resulting in the prevention of key operations. With no available workaround, the situation requires urgent attention. Example scenarios: • Single service unavailable • Loss of platform/network resilience • Backup failure • Significant degradation of service/performance
3 Major	The system is impaired, a single function is impacted but key business processes are not interrupted. Example scenarios: • Minor degradation of system performance • Single user fault
4 Minor	The problem causes minimal operational or business impact, a general technical question or enhancement request. Example scenarios: • Minor issue with no impact to service • Documentation error • Technical/product query • Enhancement request

5.3 Service Level Targets

This section describes the service milestones and the targeted service times to deliver against those milestones as set out in the Clearswift Support Agreement.

5.3.1 Service Milestones

Milestone	Description
Response	Initialisation of the support process, through engagement with the customer to progress information gathering, analysis or issue replication.
Resolution	Provision of a solution to an incident or problem, either by employing a temporary fix, an answer or a technique that provides a solution to the reported problem.
Hot Fix	Return of the user experience to the normal or expected status through implementation of a code change that resolves the incident or problem.

5.3.2 Service Targets per Milestone

Severity	Response	Response	Hot Fix
1 Critical	1 Service Hour	24 Service Hours	5 Business Days
2 High	2 Service Hours	48 Service Hours	10 Business Days
3 Major	24 Service Hours	5 Business Days	n/a
4 Minor	48 Service Hours	10 Business Days	n/a

5.3.3 Timescales

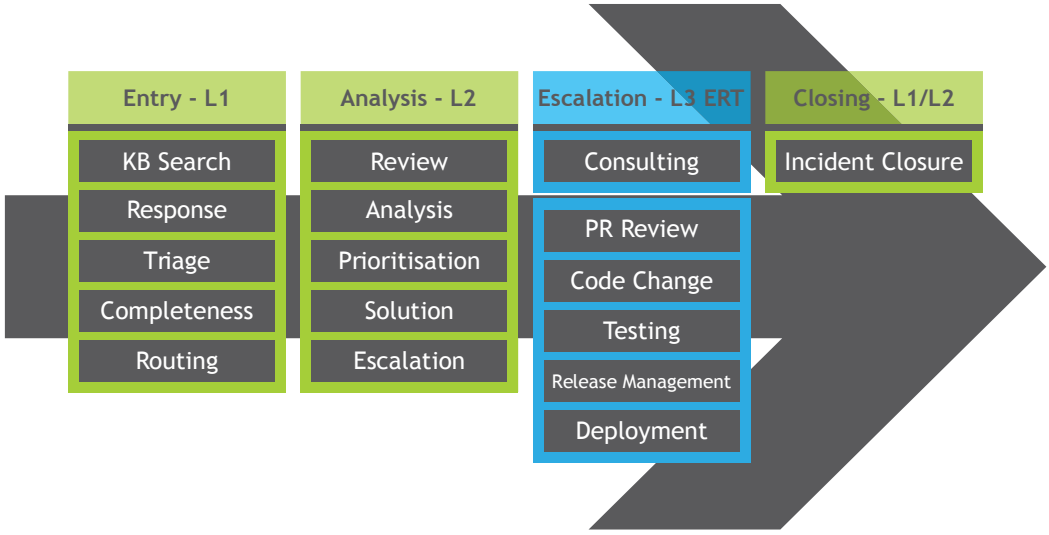
All timescales are measured from the original time and date of the incident report, unless otherwise specified. Clearswift shall monitor performance against response and resolution timescales and shall report on the percentage of incidents where these timescales are achieved within the respective target. Clearswift aim to achieve 90% compliance against these stated targets.

Note: Should Clearswift reasonably request additional information, the time periods where Clearswift are awaiting a response from the Technical Contact will be deducted from the measurement of Service Level Targets (SLTs).

Section 05: Incident Management

5.4 Incident Workflow

Support services are delivered through a tiered support model, with full visibility of functional escalation between support tiers provided to Technical Contacts through the status of the incident. The following diagram details the process flow followed during the lifecycle of an incident and the key responsibilities defined within each support tier.



5.4.1 Clearswift Application Support (Level 1)

Clearswift provides first line (L1) support for issues that can't be handled by the customer or for which customers require additional information/clarification to ensure continued system availability.

Key responsibilities include:

- Response to incidents raised by Technical Contacts
- Knowledge base searching to verify if reported problems are already known issues with a defined resolution plan
- Impact analysis with accurate classification of reported issues to ensure appropriate prioritisation
- Qualification/replication of the reported issue in an appropriate customer environment
- Initial triage to isolate unsupported 3rd party issues from potential root cause
- Information gathering to ensure complete availability of details required for root cause analysis
- Provision of technical resolution or problem workaround
- Problem routing/escalation to second/third level support or third parties where required

5.4.2 Clearswift Technical Support (Level 2)

Clearswift provides second line (L2) support, with expert Senior Technical Support professionals providing analysis and resolution of reported issues.

Key responsibilities include:

- Problem replication and diagnostic troubleshooting
- Expert assistance on product configuration and application use
- Integrated 3rd party product support
- Provision of technical resolution or problem workaround
- Defect verification with full documentation of replication environment and workflow
- Workaround analysis for identified product defects
- Defect Software Change Request (SCR) escalation
- Delivery of workarounds/fixes provided by Clearswift L3 Support

5.4.3 Clearswift Engineering Response Team (Level 3)

The Clearswift Engineering Response Team (ERT) provides third level support services for back-to-back consultation with Clearswift Technical Support, including the delivery of maintenance releases satisfying SCRs.

Key responsibilities include:

- Escalation support for unresolved second line technical support issues
- Workaround analysis for escalated product defects
- Defect resolution through the deployment of hot fixes and maintenance releases
- Defect roll-up/back-port between code branches
- Product Quality Assurance and acceptance testing
- Service availability and capacity management for hosted services
- Restoration of service outage for hosted services

5.5 Incident Lifecycle

Once a reported incident has been received by support, it is considered open until a solution has been implemented to the mutual satisfaction of both Clearswift and the customer.

Clearswift Support use the status of the incident to provide visibility of progress to Technical Contacts. Please refer to Appendix C - Incident Status for a full description of the statuses that can be assigned to an incident.

Section 05: Incident Management

5.6 Problem Management

Any problem reproduced as a generic product issue (Defect) or change request to overcome an identified functional limitation (Enhancement Request) will be reported to Clearswift Product Management via a Problem Report, documented in a knowledge base article and made visible to Clearswift customers via the customer support knowledge base on the Support Portal. The analysis of a Problem Report will result in the identification of a Software Change Request (SCR) required to deliver a resolution to a Defect or Enhancement Request.

5.6.1 Defect Processing

Once a reported problem has been qualified, reproduced and raised as a PR, customers are entitled to escalate Severity 1 and 2 PRs for resolution through the maintenance release cycle. Upon escalation, the support engineer working the incident will liaise with the Engineering Response Team (ERT) to assist in the determination of SCR priority/severity and which SCRs are to be included in a given release. The support escalation process will ensure that the Technical Contact and the relevant account personnel within Clearswift are consulted to provide input regarding the business justification for the SCR escalation. The information provided is documented against the Incident and associated PR.

5.6.2 Enhancement Request Processing

Clearswift listens to its customers. One of the best sources of information we have concerning the development of our products and features are the Enhancement Requests (ERs) that Technical Contacts submit.

An ER is any requested additional feature or function of a software program (even if originally reported as a problem). ERs raised by customers via Support are reported to Clearswift Product Management and considered for inclusion in new, future releases depending on their suitability, alignment to Clearswift product roadmap and general market trends, as well as the overall importance to the existing customer install base.

The support engineer owning the incident will work with the Technical Contact to fully document the details of the ER as well as the business need driving the request. The support engineer will then dispatch the ER to Product Management for review. ERs will be reviewed during the planning stages of each release and the status of knowledge base articles will be updated as necessary.

An incident detailing an ER shall remain open until reported to Product Management and documented for customer visibility via a knowledge base article, with the reference relayed to the Technical Contact.

5.6.3 Defect Processing

Clearswift provides a wealth of vital information via the Support Portal including product and industry documentation, FAQs and an incident driven knowledge base.

For general technical queries, troubleshooting specific issues or seeking to prevent known problems from occurring, the knowledge base is an effective resource.

The Clearswift Support knowledge base consists of articles created to enable sharing of information about known problems and their resolution, software update releases, 'how to' information, implementation tips/tricks, etc. Customers can search and view the KB articles at support.clearswift.com. A KB article will be generic to the Clearswift product, defining the problem raised, with reproducible steps and associated actions to resolve, with no reference to the customer or customer specific data.

There are three categories of KB article:

Article Type	Description
Problem Report	Defines a reproduced error in the use/function of the software/solution.
Problem Report	Defines a requested change to the functionality, performance or scope of the software/solution.
Informational	A general application, product or system specific piece of information.

Knowledge base articles will contain the following information:

- Problem definition
- Related product
- Product version (to patch level)
- Reproducible steps
- Expected/required behaviour
- Resolution/workaround
- Fix version (to patch level)

5.7 Product Downloads

The latest version of each Clearswift product, as well as relevant service packs and hot fixes, is available from the Support Portal at **www.clearswift.com/support/portals.**

Section 05: Incident Management

5.8 Escalation

Escalation is the process by which incident details are made known to other personnel for the purpose of notification or to obtain additional resources to assist in problem resolution. Escalation usually occurs when difficulties or delays are being experienced, or are considered likely, in resolving an issue.

5.8.1 Functional Escalation

The objective of functional escalation is to obtain the additional resources and expertise required to resolve a particularly difficult or complex incident. This assistance may come from L3 Engineering, 3rd party back-to-back suppliers, or from other departments within Clearswift, such as Core Development.

5.8.2 Hierarchical Escalation

The objective of hierarchical escalation is to ensure that potential problems are made known to the relevant managers and resource owners within Clearswift. This ensures the right level of focus across the organisation and the engagement of appropriate resources and expertise to expedite the resolution of customer issues. Customers can request this type of escalation if they experience or foresee delays or other problems with the resolution of issues, as set out below.

Level	Contact	Escalation Procedure
1	Technical Support Incident Owner	Support will escalate the incident on request and change the priority of the incident providing visibility to the Technical Support Manager or local Country Manager. The incident owner will contact the customer within 1 business day and agree a plan of action for progression with an agreed target timescale for communication of updates and resolution.
2	Technical Support Manager (or nominated local representative)	The Technical Support Manager or local Country Manager will be assigned as key contacts within the Escalation Team for the incident and will contact the customer within 1 business day to communicate a rescue plan for the Incident. If the problem is not resolved within target timeframe for the rescue plan, the incident shall automatically be notified to the next level of escalation.
3	Technical Support Director (or local Country Manager)	The Technical Support Director or local Country Manager will work with the Technical Support Manager and assigned Escalation Team members to determine a rescue plan for the incident, with agreed communication updates to the customer and a target resolution date. If the incident is still not resolved, the customer may request an escalation to the Chief Executive Officer. The Chief Executive Officer will contact the Customer at the earliest possible opportunity and agree a plan for resolution. The Chief Executive Officer is the final point of escalation.

5.9 Support for Third-Party Products

The Clearswift product portfolio includes and integrates with some products that are based on third-party technologies. While Clearswift provides basic first line (L1) support for these products, there may be limitations regarding the level and scope of technical support that is available.

Clearswift provides support for questions or problems related to the configuration or initial operation of the third-party products used as intended in the Clearswift product environment. Clearswift do not provide support for questions or problems arising from the use of the third-party product for non-intended uses, in non-Clearswift product environments, or in any way that violates their individual licence.

Clearswift Technical Support has the capability to escalate problems back to the vendor where necessary. This means that the turnaround time for resolution may be longer than for incidents handled exclusively by Clearswift.

5.10 Reports

Clearswift Support provides client-specific, periodic reports about incident activity. These reports include detailed information about all open and recently closed incidents and are accessible via the Support Portal at **support.clearswift.com.**

5.11 Incident Closure

When a problem has been corrected, Clearswift Support will close the incident with the agreement of the customer contact. Clearswift Support may close an incident due to any of one of the following conditions:

- The incident reported is determined to be out of scope of the Support Agreement
- A solution has been provided to resolve the incident
- Installation of a hot fix or software maintenance release has resolved the incident
- The customer contact has requested incident closure
- The product or release for which support has been requested is no longer subject to the maintenance agreement

Section 06: Service Requirements

6.1 Clearswift Obligations

1. Clearswift will provide a Service Desk function via **www.clearswift.com/support/portals**, giving specified Technical Contacts access to Clearswift Support Services during the hours specified for the service offering purchased. Customers shall report Incidents primarily via the Clearswift Support Portal but may also do so via telephone or email. This access should be used for, but not limited to:
    - Query, Problem and Defect reporting
    - Requests for general technical support
    - Requests for expert technical support to achieve issue resolution
    - Submission of Enhancement/Feature Requests
2. The Clearswift Support Portal shall be available 24x7 apart from the occasional times where the online system is down for essential maintenance.
3. Clearswift Support will work on the customer's Incident during stated service hours, excluding the days declared as public holiday close days.
4. Clearswift shall provide customers with access to the Customer Support knowledge base by access to an online service. The knowledge base shall include information on product issues raised and their resolution.
5. Clearswift shall provide each Technical Contact with individual accounts to access the Clearswift Support Portal, with sufficient privileges to enable access to all issues raised by the Customer.
6. Clearswift shall be responsible for ensuring that it has back-to-back support agreements in place with its key suppliers to ensure that it can meet the requirements specified by this agreement.
7. Clearswift shall supply to customers, on request, details of any back-to-back support agreements with third party suppliers.
8. Clearswift shall retain ownership of any problem, relating to services provided by Clearswift and assigned to them, until that problem is effectively resolved by mutual agreement.
9. Clearswift shall track and escalate problems based on the agreed 'Service Level Targets' defined in this document.

6.2 Customer Obligations

1. Customers shall formally report any Incident to Clearswift Technical Support and obtain an Incident reference number. An Incident is only tracked by Clearswift once an Incident number is issued.
2. Customers shall provide Clearswift with up-to-date contact details of their named representatives appointed as Technical Contacts for reported Incidents.
3. Customers must ensure that users of Clearswift Products and Services are suitably qualified and trained on the use of the applications.

4. Customers are responsible for the implementation of appropriate backup and recovery strategies for on premise Clearswift product, license files and data.

5. Where appropriate, customers are responsible for providing Clearswift Support with remote access to the Clearswift implementation for the purposes of problem investigation and the deployment of fixes.

6. If an Incident reported to Clearswift Support is determined to be due to the use of third party products outside of the scope of the Clearswift Support and Maintenance agreement, it is the responsibility of the customer to work with their third party supplier to resolve the issue.

7. The customer is responsible for ensuring that support fees are paid within agreed payment terms and that a valid and active Support and Maintenance agreement is in place to indicate service entitlement.

6.3 Remote Access

For on premise implementations, Customers are requested to provide Clearswift Support with external access to environments in order to aid the resolution of reported problems.

6.4 Out of Support Scope

The following services are not included within the scope of the Clearswift Support offerings:

- On-site support, unless agreed with the Clearswift Regional Technical Support Manager, as part of an active plan of action to resolve an escalation scenario
- Configuration or installation services required to implement any major or minor on premise upgrade. Such services may be provided through the purchase of Clearswift Professional Services
- Professional services, unless specified in the service offering purchased, such as, but not limited to, system audits, system benchmarking or custom report generation. These services would need to be defined and priced separately under the terms of Professional Services
- Support for on premise products that have been altered, internally adjusted, damaged or modified by the Customer without prior consent from Clearswift
- Support for the underlying platform for on premise implementations, inclusive of network and hardware/ operating system not covered under the terms of the Clearswift Support Agreement
- Support for interfaces to data sources not expressly included in the License Agreement
- Data management, data retrieval, data file copying or distribution, administration and other routine operational responsibilities
- System, software or data backup, recovery or restoration for on premise implementations

Appendix A: Web Gateway Alarm Severity

The following table details the incident severity assigned to each Web Gateway alarm.

Alarm	Severity
SMTP Inbound Transport has failed	1 Critical
SMTP Outbound Transport has failed	1 Critical
Alert handling TLS initialisation failed	2 High
Disk space is critical (data)	2 High
Disk space is critical (main)	2 High
Hardware event - disk error	2 High
Hardware event - see Hardware Event Log for details	2 High
Kaspersky Service has failed	2 High
Memory is critical	2 High
Message Area Manager has failed	2 High
Policy Engine has failed	2 High
SMTP Inbound Transport could not read the SpamLogic Database. It is recommended	2 High
Sophos Service has failed	2 High
The connection to all domain controllers has failed	2 High
Upgrade only partially completed	2 High
User Interface has failed	2 High
A supplementary license feature is no longer available	3 Major
A supplementary licensed module has failed to install	3 Major
Backup failed - see Backup Log for details	3 Major
Communications problem between this peer and the Junk Email and Malware Detection service. Please run the Connectivity Test.	3 Major
Critical Information Protection Server has failed. See Messaging Service log for more information.	3 Major
CPU usage is high for sustained period	3 Major
Failed to fetch PMM data from peer	3 Major
Failed to update LDAP address list	3 Major
Hardware event - temperature high	3 Major
IG Server unreachable. See Messaging Service log for more information.	3 Major
Illegal internal server attempting to relay	3 Major
Inbound TLS initialisation failed	3 Major
Kaspersky update failed	3 Major
LDAP Synchronization Service has failed	3 Major
Message Auditing has failed	3 Major
Missing Managers list download failed	3 Major
Outbound TLS initialisation failed	3 Major
PMM has failed	3 Major

Alarm	Severity
PMM Portal Web Server has failed	3 Major
Policy Engine error has occurred	3 Major
Policy Engine health problem detected	3 Major
Rollback operation has failed	3 Major
Service Watchdog has failed	3 Major
SQL Database has failed	3 Major
Syslog server unreachable for 30 minutes. See the Infrastructure log for more information.	3 Major
The number of messages awaiting delivery has exceeded the configured threshold	3 Major
The number of messages waiting to be processed has exceeded the configured threshold	3 Major
Transaction log export failed. See Transaction Log export Log.	3 Major
Unable to connect to at least one Domain Controller	3 Major
Unable to contact TRUST manager servers. Check your firewall settings.	3 Major
A system log file is very large	N/A
An infrastructure log file is very large	N/A
Contact your reseller or Clearswift to renew your license	N/A
Critical Information Protection Server unreachable. See Messaging Service log for more information.	N/A
Disk space is low (data)	N/A
Disk space is low (main)	N/A
Download of upgrade has failed	N/A
Failed to add audit data to database	N/A
Failed to add held message to database	N/A
Health and Statistic Gatherer has failed	N/A
Import of Encryption Certificate Store key failed. See System Services log.	N/A
Key extraction has added a disabled certificate to the Certificate Store. See the User Interface Service log for details.	N/A
Managed list download failed	N/A
Memory is low	N/A
Policy Engine failed to move a message	N/A
Policy Engine failed to process a message	N/A
Post-upgrade task in progress	N/A
Restore completed successfully	N/A
Restore failed - see Backup Log for details	N/A
Restore interrupted - see Backup Log for details	N/A
SMTP Alert Transport has failed	N/A
Sophos update has failed	N/A
This upgrade may not be uninstalled	N/A
Upgrade has failed	N/A
Update is available	N/A

Appendix B: Email Gateway Alarm Severity

The following table details the incident severity assigned to each Email Gateway alarm.

Alarm	Severity
Exchange Message Transport Server has failed. See the Exchange Message Transport Server log.	1 Critical
Disk space is critical (data)	2 High
Disk space is critical (main)	2 High
Hardware event - disk error	2 High
Hardware event - see Hardware Event Log for details	2 High
Kaspersky Service has failed	2 High
Memory is critical	2 High
Message Area Manager has failed	2 High
Policy Engine has failed	2 High
Sophos Service has failed	2 High
The connection to all domain controllers has failed	2 High
Upgrade only partially completed	2 High
User Interface has failed	2 High
A supplementary license feature is no longer available	3 Major
A supplementary licensed module has failed to install	3 Major
Attempted access by unregistered Exchange Interceptor. See the Exchange Message Transport Server log.	3 Major
Backup failed - see Backup Log for details	3 Major
Critical Information Protection Server has failed. See Messaging Service log for more information.	3 Major
CPU usage is high for sustained period	3 Major
Failed to fetch PMM data from peer	3 Major
Failed to update LDAP address list	3 Major
Hardware event - temperature high	3 Major
IG Server unreachable. See Messaging Service log for more information.	3 Major
Kaspersky update failed	3 Major
LDAP Synchronization Service has failed	3 Major
Message Auditing has failed	3 Major
Missing Managers list download failed	3 Major
PMM has failed	3 Major
PMM Portal Web Server has failed	3 Major
Policy Engine error has occurred	3 Major
Policy Engine health problem detected	3 Major
Rollback operation has failed	3 Major
Service Watchdog has failed	3 Major
SQL Database has failed	3 Major

Alarm	Severity
Syslog server unreachable for 30 minutes. See the Infrastructure log for more information.	3 Major
The number of messages awaiting delivery has exceeded the configured threshold	3 Major
The number of messages waiting to be processed has exceeded the configured threshold	3 Major
Transaction log export failed. See Transaction Log export Log.	3 Major
Unable to connect to at least one Domain Controller	3 Major
A system log file is very large	N/A
An infrastructure log file is very large	N/A
Contact your reseller or Clearswift to renew your license	N/A
Critical Information Protection Server unreachable. See Messaging Service log for more information.	N/A
Disk space is low (data)	N/A
Disk space is low (main)	N/A
Download of upgrade has failed	N/A
Failed to add audit data to database	N/A
Failed to add held message to database	N/A
Health and Statistic Gatherer has failed	N/A
Managed list download failed	N/A
Memory is low	N/A
Policy Engine failed to move a message	N/A
Policy Engine failed to process a message	N/A
Post-upgrade task in progress	N/A
Restore completed successfully	N/A
Restore failed - see Backup Log for details	N/A
Restore interrupted - see Backup Log for details	N/A
SMTP Alert Transport has failed	N/A
Sophos update has failed	N/A
The number of messages awaiting retrieval by the Exchange Interceptors has exceeded the configured threshold. See the Exchange Message Transport Server log and check the state of the Exchange Interceptors.	N/A
This upgrade may not be uninstalled	N/A
Upgrade has failed	N/A
Update is available	N/A
Restore failed - see Backup Log for details	N/A
Restore interrupted - see Backup Log for details	N/A
SMTP Alert Transport has failed	N/A
Update is available	N/A

Appendix C: ARgon for Email Alarm Severity

The following table details the incident severity assigned to each ARgon for Email.

Alarm	Severity
SMTP Inbound Transport has failed	1 Critical
SMTP Outbound Transport has failed	1 Critical
Alert handling TLS initialisation failed	2 High
Disk space is critical (data)	2 High
Disk space is critical (main)	2 High
Hardware event - disk error	2 High
Hardware event - see Hardware Event Log for details	2 High
Memory is critical	2 High
Message Area Manager has failed	2 High
Policy Engine has failed	2 High
The connection to all domain controllers has failed	2 High
User Interface has failed	2 High
A supplementary license feature is no longer available	3 Major
A supplementary licensed module has failed to install	3 Major
Backup failed - see Backup Log for details	3 Major
Critical Information Protection Server has failed. See Messaging Service log for more information.	3 Major
CPU usage is high for sustained period	3 Major
Failed to update LDAP address list	3 Major
Hardware event - temperature high	3 Major
Illegal internal server attempting to relay	3 Major
Inbound TLS initialisation failed	3 Major
LDAP Synchronization Service has failed	3 Major
Message Auditing has failed	3 Major
Missing Managers list download failed	3 Major
Outbound TLS initialisation failed	3 Major
Policy Engine error has occurred	3 Major
Policy Engine health problem detected	3 Major
Service Watchdog has failed	3 Major
SQL Database has failed	3 Major
Syslog server unreachable for 30 minutes. See the Infrastructure log for more information.	3 Major
The number of messages awaiting delivery has exceeded the configured threshold	3 Major
The number of messages waiting to be processed has exceeded the configured threshold	3 Major

Alarm	Severity
Transaction log export failed. See Transaction Log export Log.	3 Major
Unable to connect to at least one Domain Controller	3 Major
A system log file is very large	N/A
An infrastructure log file is very large	N/A
Contact your reseller or Clearswift to renew your license	N/A
Critical Information Protection Server unreachable. See Messaging Service log for more information.	N/A
Disk space is low (data)	N/A
Disk space is low (main)	N/A
Failed to add audit data to database	N/A
Failed to add held message to database	N/A
Health and Statistic Gatherer has failed	N/A
Import of Encryption Certificate Store key failed. See System Services log	N/A
Key extraction has added a disabled certificate to the Certificate Store. See the User Interface Service log for details.	N/A
Managed list download failed	N/A
Memory is low	N/A
Policy Engine failed to move a message	N/A
Policy Engine failed to process a message	N/A
Restore completed successfully	N/A
Restore failed - see Backup Log for details	N/A
Restore interrupted - see Backup Log for details	N/A
SMTP Alert Transport has failed	N/A
Upgrade is available	N/A

HelpSystems, LLC. All trademarks and registered trademarks are the property of their respective owners. | www.clearswift.com

Appendix D: Web Gateway Alarm Severity

The following table details the incident severity assigned to each Web Gateway alarm.

Alarm	Severity
Web Proxy has failed	1 Critical
Disk space is critical (data)	2 High
Disk space is critical (main)	2 High
Hardware event - disk error	2 High
Hardware event - see Hardware Event Log for details	2 High
HTTPS Certificate Master Server not available	2 High
Infrastructure service has failed	2 High
Kaspersky Service has failed	2 High
Memory is critical	2 High
Sophos Service has failed	2 High
The connection to all domain controllers has failed	2 High
The dedicated disk used for caching has failed or is missing. Please reconfigure your cache disk settings.	2 High
Upgrade only partially completed	2 High
User authentication service has failed	2 High
User Interface has failed	2 High
Web Auditor service has failed	2 High
A content scanning engine was restarted as it was unable to process a job.	3 Major
A supplementary license feature is no longer available	3 Major
A supplementary licensed module has failed to install	3 Major
Backup failed - see Backup Log for details	3 Major
Critical Information Protection Server has failed. See Messaging Service log for more information.	3 Major
CPU usage is high for sustained period	3 Major
Error occured while reading the proxy configuration	3 Major
Failed to transfer Web Audit logs	3 Major
Failed to update LDAP address list	3 Major
Hardware event - temperature high	3 Major
IG Server unreachable. See Messaging Service log for more information.	3 Major
Kaspersky update has failed	3 Major
LDAP Synchronization Service has failed	3 Major
Possible reverse DNS problem has been detected. See the Web Proxy Events log for more information.	3 Major
Problem processing Web Audit data	3 Major
Proxifier log too big	3 Major
Proxy HTTPS certificate was not installed. See System Services log.	3 Major

Alarm	Severity
Revoked Certificates download failed	3 Major
Rollback operation has failed	3 Major
Service Watchdog has failed	3 Major
SQL Database has failed	3 Major
Syslog server unreachable for 30 minutes. See the Infrastructure log for more information.	3 Major
The Remote User Service has failed	3 Major
The malware URL database is out of date	3 Major
The phishing URL database is out of date	3 Major
The URL database is out of date	3 Major
Transaction log export failed. See Transaction Log export Log.	3 Major
URL database could not be loaded	3 Major
Web Proxy has failed and was restarted	3 Major
A content scanning engine is unable to process a job.	N/A
A system log file is very large	N/A
A Web Proxy log file is very large	N/A
An infrastructure log file is very large	N/A
Contact your reseller or Clearswift to renew your license	N/A
Critical Information Protection Server unreachable. See Messaging Service log for more information.	N/A
Disk space is low (data)	N/A
Disk space is low (main)	N/A
Download of upgrade has failed	N/A
Health and Statistic Gatherer has failed	N/A
Mail Alert Transport has failed	N/A
Managed list download failed	N/A
Memory is low	N/A
Post-upgrade task in progress	N/A
Restore completed successfully	N/A
Restore failed - see Backup Log for details	N/A
Restore interrupted - see Backup Log for details	N/A
SMTP Alert Transport has failed	N/A
Sophos update has failed	N/A
The Caic URL database is out of date	N/A
The Web Proxy diagnostics directory is very large	N/A
The Web Proxy requests directory is very large	N/A
This upgrade may not be uninstalled	N/A
Upgrade has failed	N/A
Upgrade is available	N/A

Appendix E: ICAP Gateway Alarm Severity

The following table details the incident severity assigned to each ICAP Gateway alarm.

Alarm	Severity
Web Proxy has failed	1 Critical
Disk space is critical (data)	2 High
Disk space is critical (main)	2 High
Hardware event - disk error	2 High
Hardware event - see Hardware Event Log for details	2 High
HTTPS Certificate Master Server not available	2 High
Infrastructure service has failed	2 High
Kaspersky Service has failed	2 High
Memory is critical	2 High
Sophos Service has failed	2 High
The connection to all domain controllers has failed	2 High
The dedicated disk used for caching has failed or is missing. Please reconfigure your cache disk settings.	2 High
Upgrade only partially completed	2 High
User authentication service has failed	2 High
User Interface has failed	2 High
Web Auditor service has failed	2 High
A content scanning engine was restarted as it was unable to process a job.	3 Major
A supplementary license feature is no longer available	3 Major
A supplementary licensed module has failed to install	3 Major
Backup failed - see Backup Log for details	3 Major
Critical Information Protection Server has failed. See Messaging Service log for more information.	3 Major
CPU usage is high for sustained period	3 Major
Error occured while reading the proxy configuration	3 Major
Failed to transfer Web Audit logs	3 Major
Failed to update LDAP address list	3 Major
Hardware event - temperature high	3 Major
IG Server unreachable. See Messaging Service log for more information.	3 Major
Kaspersky update has failed	3 Major
LDAP Synchronization Service has failed	3 Major
Possible reverse DNS problem has been detected. See the Web Proxy Events log for more information.	3 Major
Problem processing Web Audit data	3 Major
Proxifier log too big	3 Major
Proxy HTTPS certificate was not installed. See System Services log.	3 Major

Alarm	Severity
Disk space is critical (data)	2 High
Disk space is critical (main)	2 High
Hardware event - disk error	2 High
Hardware event - see Hardware Event Log for details	2 High
Infrastructure service has failed	2 High
Kaspersky Service has failed	2 High
Memory is critical	2 High
Sophos Service has failed	2 High
The connection to all domain controllers has failed	2 High
The dedicated disk used for caching has failed or is missing. Please reconfigure your cache disk settings.	2 High
The ICAP Server has failed	2 High
Upgrade only partially completed	2 High
User Interface has failed	2 High
A content scanning engine was restarted as it was unable to process a job.	3 Major
A supplementary license feature is no longer available	3 Major
A supplementary licensed module has failed to install	3 Major
Backup failed - see Backup Log for details	3 Major
Critical Information Protection Server has failed. See Messaging Service log for more information.	3 Major
CPU usage is high for sustained period	3 Major
Error occured while reading the ICAP Server configuration	3 Major
Failed to transfer Web Audit logs	3 Major
Failed to update LDAP address list	3 Major
Hardware event - temperature high	3 Major
IG Server unreachable. See Messaging Service log for more information.	3 Major
Kaspersky update has failed	3 Major
LDAP Synchronization Service has failed	3 Major
Possible reverse DNS problem has been detected. See the Web Proxy Events log for more information.	3 Major
Problem processing Audit data	3 Major
Rollback operation has failed	3 Major
Service Watchdog has failed	3 Major
SQL Database has failed	3 Major
Syslog server unreachable for 30 minutes. See the Infrastructure log for more information.	3 Major
The malware URL database is out of date	3 Major
The phishing URL database is out of date	3 Major
The URL database is out of date	3 Major
Upgrade has failed	N/A
Upgrade is available	N/A

Appendix F: Incident Status

The following table details the statuses that can be assigned to an incident.

Milestone	Description
New	The incident is currently queued with a 1st line support agent, awaiting response.
Under Analysis L1	The incident has been responded to and is currently being worked by the L1 Support tier.
Under Analysis L2	The incident has been escalated to L2 Subject Matter Expert for troubleshooting and root cause analysis.
Under Analysis L3	The incident has been escalated to the L3 Engineering Response Team (ERT) for consultation.
Under Analysis 3rd party	The incident has been escalated to a third party for back-to-back support for integrated components.
Hot Fix Escalated	A Critical/High severity problem is escalated, with an associated SCR to be resolved through delivery of an emergency patch.
Contact Input Received	The Technical Contact has updated the case via web comment or email.
NOTE: SLA reporting excludes all time under the following status values	
Awaiting Customer	The action is on the customer to respond to the request that has been made. This may be to provide additional information. The customer is notified via email of any incident that has been changed to this action.
Awaiting Solution Confirmation	An answer/solution has been provided, waiting for customer verification of resolution.
Awaiting HF Confirmation	Hot fix was delivered, waiting for verification of resolution.
Awaiting Patch Confirmation	Software update delivered, waiting for verification of resolution.
Awaiting Future Handling	Incident handling is deferred, the customer agrees to suspend the SLA clock and postpone the request.
Awaiting 3rd Party	The incident is escalated to a 3rd party with no back-to-back SLA in place.
Awaiting PR Review	A Major/Minor severity Problem Report has been raised with ERT pending review.
Awaiting ER Review	An Enhancement Request has been raised with Product Management pending review.
Awaiting Patch	Problem resolution is targeted for a scheduled maintenance release.
Awaiting Work Request	Problem resolution is dependent upon a service engagement which needs to be scheduled under standard consulting service process.
Awaiting Scheduled Maintenance	The incident will be resolved through planned maintenance.
Closed	The incident is closed.

clearswift
by HelpSystems

www.clearswift.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.

HelpSystems, LLC. All trademarks and registered trademarks are the property of their respective owners.

(S02-CSH-21)