SecureLogix® Call Secure™ Managed Service

Operations Guide

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 • (210) 402-9669 • securelogix.com

Support: (877) SLC-4HELP • EMAIL support@securelogix.com • support.securelogix.com

Table of Contents

1. Introduction

1.1. Purpose

The purpose of this document is to provide an overview of the operational workflow regarding policy-based incident response and customer initiated requests for your SecureLogix® Call Secure™ Managed Service.

1.2. Related Documents

SecureLogix® Call Secure™ Managed Security Service for Voice Statement of Work—Please reference your SOW for specifics on what is included in the managed service.

2. Customer Contact Requirements

Requests for policy updates or reports can only be initiated by the customer-specified contacts provided during the onboarding phase of the managed service.

3. SecureLogix Service Information

3.1. Service Hours

Service hours are Monday through Friday from 8:00 AM to 5:00 PM Central Time (exclusive of holidays listed at SecureLogix_Holidays).

3.2. Contacting the Services Team

All requests/questions must be sent to the following email address. For policy block requests, please provide the information outlined in the Block Request Template below.

Email: - managedservices@securelogix.com

Block Request Template:

Phone number(s) that you want to be blocked:
+12101111111

Number(s) Category:
<Fraud> or <Harassing>

Business Case and Description:
Continues to call multiple times per day. Making threats to agents.

Report Request Template:

Please provide specifics for report filtering such as:

- Phone numbers, are they internal or external, call direction (inbound, outbound, both)
- Report period, start and end date

- Recurrence (one time, weekly, monthly, etc..)
- Report recipients

Note: An email received by the address above will automatically generate a managed service case and the sender will receive a response email with the corresponding case number.

3.3. Service Delivery Objectives

3.3.1.Service Action Request

- Service Action Requests will be acknowledged within one hour during business hours.
- Service Action Requests received outside of business hours will be acknowledged the next business day.
- Service Action Requests are generally completed within four business hours of receipt of the request; however, in all cases, requests will be completed by the end of the next business day following receipt of the request.

3.3.2. Incident Response

- SecureLogix will notify the customer of critical security policy alert threshold violations within one hour during business hours.
- For security policy alerts and incidents occurring outside of the defined Incident Response Service Hours, SecureLogix will notify the customer on a best-effort basis, but in all cases no later than the next business day**.**

3.4. Escalation Contact Information

If you are experiencing issues with the delivery of the SecureLogix Managed Service, please contact:

Ricky Crow
Manager, SecureLogix Managed Services
+1-210-546-1055 direct
rcrow@securelogix.com

4. Policy Management

4.1. Firewall Policy

The services team will maintain the firewall policy based on customer requirements. We will provide best-practices recommendations based on daily monitoring and monthly reporting.

The firewall policy is subject to change daily based on day-to-day operations and requirements. A case will be opened in the SecureLogix Salesforce Case system for each action requests and an action request authorization will be required from the documented customer-approved list of Authorization personnel. Once the authorization has been received, the analyst will implement the request in accordance with the directions specified by the requestor.. Once completed, the analyst will notify the customer to confirm the request has been implemented.

4.2. Intrusion Prevention Policy (IPS)

The services team will maintain the IPS policy based on the customer requirements. We will also provide best-practices recommendations based on calling pattern thresholds over an agreed-upon interval. The initial thresholds will be established through a series of baseline reporting, analysis, and discussion with the customer. When a threshold is breached, the services team will investigate by running the appropriate reports and analyzing the data. The analysts will summarize the findings and provide them to the customer along with any recommendations.

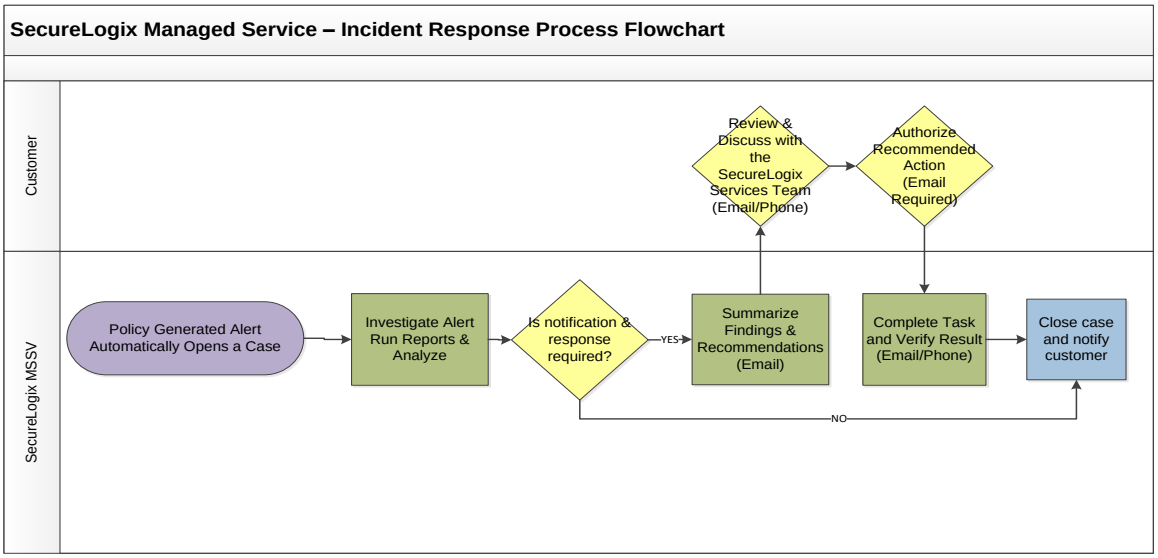
The IPS policy is subject to change daily based on day-to-day operations and requirements. A case will be opened in the SecureLogix Salesforce Case system for each action requests and an authorization will be required from the documented customer-approved list of Authorization personnel. Once the authorization has been received, the analyst will implement the request in accordance with the directions specified by the requestor.. Once completed, the analyst will notify the customer to confirm the request has been implemented.

5. Operational Workflow

5.1. Policy Based Events

The services team will provide proactive monitoring and response to alerts generated by the system policies. If any of the rules in the customer's security policy are triggered and require reporting, analysis, and/or intervention, the services team will respond and take appropriate action with customer approval.

The chart below outlines the process followed when a policy-based alert is received.


SecureLogix Managed Service – Incident Response Process Flowchart
Customer
SecureLogix MSSV
Policy Generated Alert Automatically Opens a Case
Investigate Alert Run Reports & Analyze
Is notification & response required?
YES
NO
Summarize Findings & Recommendations (Email)
Review & Discuss with the SecureLogix Services Team (Email/Phone)
Authorize Recommended Action (Email Required)
Complete Task and Verify Result (Email/Phone)
Close case and notify customer

5.2. Customer Initiated Request or Reported Incident

When requesting support, please remember to:

- Provide as much detailed information about the issue or situation as possible.
  - Many times, there will be several ways to resolve an issue or present in a report, so providing details will help the analyst determine the best way to support the request.
- If the request is time-sensitive, please tag it as “High Priority.” This can be in the subject line or body of the email.

The chart below outlines the process followed when the customer initiates a request.