



Silent Push Installation and Configuration Guide

Software Version 1.0

Integration Guide

February 22, 2024



©2023 ThreatConnect, Inc.

ThreatConnect® is a registered trademark, and TC Exchange™ is a trademark, of ThreatConnect, Inc.



Table of Contents

Overview	5
Dependencies	6
ThreatConnect Dependencies	6
Silent Push Dependencies	6
Application Installation and Configuration	6
Available Actions Explained	6
Domain Enrichment	6
Configuration Parameters.....	7
Domain Search.....	8
Configuration Parameters.....	8
Domain Typosquatting Search.....	9
Configuration Parameters.....	10
Forward PADNS Lookup.....	13
Configuration Parameters.....	13
Get ASN Reputation.....	17
Configuration Parameters.....	17
Get ASN Reputation History.....	18
Configuration Parameters.....	18
Get ASN Takedown Reputation.....	19
Configuration Parameters.....	19
Get ASN Takedown Reputation History.....	19
Configuration Parameters.....	20
Get Bulk Domain Information.....	20
Configuration Parameters.....	20
Get Bulk Domain Risk Score.....	21
Configuration Parameters.....	21
Get Bulk IPv4 History Information.....	22
Configuration Parameters.....	22
Get Bulk IPv4 Information.....	22
Configuration Parameters.....	23
Get Bulk IPv4 Risk Score.....	23
Configuration Parameters.....	23
Get Cousin Domains.....	24
Configuration Parameters.....	24
Get Nameserver Reputation.....	24
Configuration Parameters.....	24
Get Nameserver Reputation History.....	25
Configuration Parameters.....	25



Get Sibling Domains.....	26
Configuration Parameters.....	26
Get Subnet Reputation.....	26
Configuration Parameters.....	27
Get Subnet Reputation History.....	27
Configuration Parameters.....	27
IPv4 Enrichment.....	28
Configuration Parameters.....	28
Multicondition PADNS Lookup.....	29
Configuration Parameters.....	29
Reverse PADNS Lookup.....	32
Configuration Parameters.....	33
Advanced Request.....	36
Configuration Parameters.....	36
Frequently Asked Questions (FAQ).....	38



Overview

The ThreatConnect® integration with Silent Push allows users to query the SilentPush API endpoints listed below:

- Enrichments
- Domain
- IPV4
- Reputation
- PADNS

There are 23 available actions that can be performed and they are listed as follows:

1. Domain Enrichment
2. Domain Search
3. Domain Typosquatting Search
4. Forward PADNS Lookup
5. Get ASN Reputation
6. Get ASN Reputation History
7. Get ASN Takedown Reputation
8. Get ASN Takedown Reputation History
9. Get Bulk Domain Information
10. Get Bulk Domain Risk Score
11. Get Bulk IPv4 History Information
12. Get Bulk IPv4 Information
13. Get Bulk IPv4 Risk Score
14. Get Cousin Domains
15. Get Nameserver Reputation
16. Get Nameserver Reputation History
17. Get Sibling Domains
18. Get Subnet Reputation
19. Get Subnet Reputation History
20. IPv4 Enrichment
21. Multicondition PADNS Lookup
22. Reverse PADNS Lookup
23. Advanced Request



Dependencies

ThreatConnect Dependencies

- ThreatConnect instance with version 7.4.0 or newer installed

Note: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Customers on Dedicated Cloud and On-Premises instances can enable these settings on the **Account Settings** screen within their ThreatConnect instance.

Silent Push Dependencies

- SilentPush API Key

Application Installation and Configuration

1. Log into ThreatConnect with a System Administrator account.
2. Install the **Silent Push** App via TC Exchange™.
3. Insert the **Silent Push** App into any Playbook

Available Actions Explained

Domain Enrichment

Gets the domain enrichment information related to the domain age, the NS reputation, the active period, historical listings, etc.

For more information, please visit the Silent Push API documentation:



<https://docs.silentpush.com/enrich.html#domain-enrichment>

Configuration Parameters

Table 1

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Domain	The domain that is being sent to Silent Push for enrichment.	String	Yes
Explain	Show details of data used to calculate the different scores in the response. <ul style="list-style-type: none">• False (default)<ul style="list-style-type: none">○ Do not show details• True<ul style="list-style-type: none">○ Show underlying data used to calculated scores	Boolean	No
Scan Data	Show details of data collected from host scanning <ul style="list-style-type: none">• False (default)<ul style="list-style-type: none">○ Do not show details• True<ul style="list-style-type: none">○ Show collected data	Boolean	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No



Domain Search

Capability to search for domains that match specific parameters. 10 common parameters are listed below. Enhance your search by adding optional query parameters. Additional parameters that can be used are listed here:

<https://docs.silentpush.com/domain.html#domain-search>.

Configuration Parameters

Table 2

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
asn	Search for IP addresses in or not in the given AS numbers <ul style="list-style-type: none">in (default)notin	String	No
asn_diversity_min	Minimum diversity limit number	String	No
domain	The domain that is being sent to Silent Push for enrichment.	String	No
domain_regex	RE2 regular expression - overrides domain parameter	String	No
first_seen_min	yyyy-mm-dd <ul style="list-style-type: none">Only domains that have A records seen for the first time after the given date	String	No
ip_diversity_all_min	minimum diversity limit <ul style="list-style-type: none">default = 1	String	No



last_seen_min	yyyy-mm-dd <ul style="list-style-type: none">only domains that have A records last seen more recently than the given date	String	No
network	subnet	String	No
nsname	Name server name or wildcard pattern of name server used by domains <ul style="list-style-type: none">use nsname=self to find domains hosting their own nameservers	String	No
registrar	Only domains registered using this registrar Partial string match, or any if not set	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Domain Typosquatting Search

Capability to find typosquatting variations of domains. Enhance your search by adding optional query parameters. 10 common parameters are listed below. Enhance your search by adding optional query parameters. Additional parameters that can be used are listed here: <https://docs.silentpush.com/domain.html#domain-typosquatting-search>.

The default is to view new records from the past 7 days, but this can be narrowed to the last 24 hours for a daily search. Only records that have been seen within the last 7 days will be considered in this search.



Configuration Parameters

Table 3

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
autospoof	domain name for which to find spoofed variations <ul style="list-style-type: none">• automatically generates a regex used in search• is overridden by the regex parameter, if given	String	No
first_seen_after	< date or epoch or sec or period > <ul style="list-style-type: none">• first_seen timestamp must be on or after this time<ul style="list-style-type: none">○ default=-2592000 - look back 30 days○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time < sec > seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time < nX > ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : months	String	No
first_seen_before	< date or epoch or sec or period >	String	No



	<ul style="list-style-type: none">● first_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time < sec > seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time < nX > ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : months		
last_seen_after	< date or epoch or sec or period > <ul style="list-style-type: none">● last_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time < sec > seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time < nX > ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : month	String	No
last_seen_before	< date or epoch or sec or period > <ul style="list-style-type: none">● last_seen timestamp must be on or after this time	String	No



	<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time < sec > seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time < nX > ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : month		
match	<p>< eq or noteq ></p> <p>finds domains not on (neq) or on (eq) name servers given as nsname parameters</p> <ul style="list-style-type: none">● neq (default) - domains not on name servers● eq - domains on name servers	String	No
net	<p>< in or notin ></p> <p>find records where ip not in (default) or in subnet defined by netmask and additional network parameters</p> <ul style="list-style-type: none">● notin (default) - find records not in subnet● in - find records in subnet	String	No
network	<p>< subnet ></p> <ul style="list-style-type: none">● additional network and net mask● give option as 1.1.1/24● up to 5 additional networks may be given	String	No
nsname	<p>< name or pattern ></p>	String	No



	finds domains not on (neq) or on (eq) name servers given as nsname parameters <ul style="list-style-type: none">• neq (default) - domains not on name servers• eq - domains on name servers		
regex	< pattern > re2 regular expression <ul style="list-style-type: none">• pattern must be a valid re2 regular expression• regex overrides any autospoof domain given	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbo x	No

Forward PADNS Lookup

Capability to do a forward lookup of Passive DNS data. 7 common parameters are listed below. Enhance your search by adding optional query parameters. Additional parameters that can be used are listed here: <https://docs.silentpush.com/padns.html#forward-padns-lookup>.

Configuration Parameters

Table 4

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Query Type	The following query types are supported: <ul style="list-style-type: none">• a• aaaa	String	Yes



	<ul style="list-style-type: none">• cname• mx• ns• ptr4• ptr6• any• anyipv4• anyipv6• soa• txt		
Query Name	Specify a name or IP address to lookup <ul style="list-style-type: none">• <i>name - wildcards (*)</i> are supported in name string• IPv4• IPv6	String	Yes
first_seen_after	< date or epoch or sec or period > <ul style="list-style-type: none">• first_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : months	String	No



first_seen_before	<p>< date or epoch or sec or period ></p> <ul style="list-style-type: none">• first_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : months	String	No
last_seen_after	<p>< date or epoch or sec or period ></p> <ul style="list-style-type: none">• last_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago	String	No



	<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : month		
last_seen_before	<p>< date or epoch or sec or period ></p> <ul style="list-style-type: none">● last_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : month	String	No
netmask	<p>Net mask may be given for query types ptr4 or ptr6</p> <ul style="list-style-type: none">● defaults: IPv4 = 32, IPv6 = 128	String	No
regex	<p>re2 regular expression</p> <ul style="list-style-type: none">● pattern must be a valid re2 regular expression	String	No



subdomains	Include or exclude subdomains from qtype a or aaaa results <ul style="list-style-type: none">• 0 = exclude• 1 = include	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get ASN Reputation

Capability to get information about ASN reputation. Input should only be numeric, without AS or ASN prefix.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/reputation.html#asn-takedown-reputation>

Configuration Parameters

Table 5

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
ASN	ASN number without AS or ASN prefix	String	Yes
Explain	Show information used to calculate the reputation score <ul style="list-style-type: none">• 0 = (default) do not show• 1 = show details	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave	Checkbox	No



	the box unchecked if no failure is required when the response is empty.		
--	---	--	--

Get ASN Reputation History

Capability to get ASN reputation history. Input should only be numeric, without AS or ASN prefix.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/reputation.html#asn-takedown-reputation-history>

Configuration Parameters

Table 6

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
ASN	ASN number without AS or ASN prefix	String	Yes
Explain	Show information used to calculate the reputation score <ul style="list-style-type: none">• 0 = (default) do not show• 1 = show details	String	No
Limit	Integer number of results to return	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No



Get ASN Takedown Reputation

Capability to get ASN takedown reputation. Input should only be numeric, without AS or ASN prefix.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/reputation.html#asn-takedown-reputation>

Configuration Parameters

Table 7

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
ASN	ASN number without AS or ASN prefix	String	Yes
Explain	Show information used to calculate the reputation score <ul style="list-style-type: none">• 0 = (default) do not show• 1 = show details	String	No
Limit	Integer number of results to return	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get ASN Takedown Reputation History

Capability to get ASN takedown reputation history. Input should only be numeric, without AS or ASN prefix.

For more information, please visit the Silent Push API documentation:



<https://docs.silentpush.com/reputation.html#asn-takedown-reputation-history>

Configuration Parameters

Table 8

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
ASN	ASN number without AS or ASN prefix	String	Yes
Explain	Show information used to calculate the reputation score <ul style="list-style-type: none">• 0 = (default) do not show• 1 = show details	String	No
Limit	Integer number of results to return	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get Bulk Domain Information

Capability to bulk search information for multiple domains.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/domain.html#bulk-domain-information>

Configuration Parameters

Table 9

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes



Domains	A string array containing a list of domains "Domain1, Domain2, Domain3"	StringArray	Yes
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get Bulk Domain Risk Score

Capability to bulk search for silent push risk scores for multiple domains.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/domain.html#bulk-silent-push-risk-score-for-a-list-of-domains>

Configuration Parameters

Table 10

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Domains	A string array containing a list of domains "Domain1, Domain2, Domain3"	StringArray	Yes
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No



Get Bulk IPv4 History Information

Capability to get bulk historical information for a list of IPv4 addresses for one or multiple dates. This information is valuable for tracking the network infrastructure and changes related to the IP addresses over time.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/ipv4.html#bulk-ipv4-history-information>

Configuration Parameters

Table 11

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
IPv4 Addresses	"ip1,ip2,ip3"	StringArray	Yes
Dates	"yyyymmdd, yyyymmdd, yyyymmdd"	StringArray	Yes
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get Bulk IPv4 Information

Capability to bulk search information for multiple IPv4 addresses.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/ipv4.html#bulk-ipv4-information>



Configuration Parameters

Table 12

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
IPv4 Addresses	"ip1,ip2,ip3"	StringArray	Yes
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get Bulk IPv4 Risk Score

Capability to bulk search for silent push risk scores for multiple IPv4 addresses.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/ipv4.html#bulk-silent-push-risk-score-for-a-list-of-ipv4-addresses>

Configuration Parameters

Table 13

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
IPv4 Addresses	"ip1,ip2,ip3"	StringArray	Yes
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No



Get Cousin Domains

Capability to find out the cousin domains of a domain. A cousin domain is a domain that looks deceptively similar to a legitimate target domain.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/domain.html?highlight=cousin#cousin-domains>

Configuration Parameters

Table 14

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Domain	Domain	String	Yes
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get Nameserver Reputation

Capability to get name server reputation.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/reputation.html#name-server-reputation>

Configuration Parameters

Table 15

Name	Description	Type	Required?
------	-------------	------	-----------



API Key	Silent Push API key	String	Yes
Nameserver	Name server - ns-380.awsdns-47.com	String	Yes
Explain	Show information used to calculate the reputation score <ul style="list-style-type: none">• 0 = (default) do not show• 1 = show details	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get Nameserver Reputation History

Capability to get name server reputation history.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/reputation.html#name-server-reputation-history>

Configuration Parameters

Table 16

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Nameserver	Name server - ns-380.awsdns-47.com	String	Yes
Explain	Show information used to calculate the reputation score <ul style="list-style-type: none">• 0 = (default) do not show• 1 = show details	String	No
Limit	Integer limit of results to return	String	No



Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No
--------------------	--	----------	----

Get Sibling Domains

Capability to find out the sibling domains of a domain. A sibling domain is an exact replica of a primary domain, in all respects except the name of the domain itself.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/domain.html#sibling-domains>

Configuration Parameters

Table 17

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Domain	Domain	String	Yes
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get Subnet Reputation

Capability to get IPv4 Subnet reputation.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/reputation.html?highlight=nameserver%20reputation#subnet-reputation>



Configuration Parameters

Table 18

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Subnet	IPV4 Subnet	String	Yes
Mask	Subnet Mask	String	Yes
Explain	Show information used to calculate the reputation score <ul style="list-style-type: none">• 0 = (default) do not show• 1 = show details	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Get Subnet Reputation History

Capability to get IPv4 Subnet reputation history.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/reputation.html#subnet-reputation-history>

Configuration Parameters

Table 19

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Subnet	IPV4 Subnet	String	Yes



Mask	Subnet Mask	String	Yes
Explain	Show information used to calculate the reputation score <ul style="list-style-type: none">• 0 = (default) do not show• 1 = show details	String	No
Limit	Integer number of results to return	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

IPv4 Enrichment

IPv4 enrichment information related to the Autonomous System Number, IP characteristics, risk score, etc.

For more information, please visit the Silent Push API documentation:

<https://docs.silentpush.com/enrich.html#ipv4-enrichment>

Configuration Parameters

Table 20

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
IPv4 Address	IPV4 Address	String	Yes
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No



Multicondition PADNS Lookup

Capability to do a lookup of Passive DNS data based on a query. 7 common parameters are supplied automatically. Enhance your search by adding optional query parameters by referencing: <https://docs.silentpush.com/padns.html#multi-condition-padns-lookup>.

Configuration Parameters

Table 21

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Query Type	The following query types are supported: <ul style="list-style-type: none">• a• aaaa• cname• mx• ns• ptr4• ptr6	String	Yes
Query Name	Specify a name or IP address to lookup <ul style="list-style-type: none">• <i>name - wildcards (*)</i> are supported in name string• IPv4• IPv6	String	Yes
Query Answer	Specify a name or IP address to lookup <ul style="list-style-type: none">• <i>name - wildcards (*)</i> are supported in name string• IPv4• IPv6	String	Yes
first_seen_after	< date or epoch or sec or period >	String	No



	<ul style="list-style-type: none">• first_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : months		
first_seen_before	< date or epoch or sec or period > <ul style="list-style-type: none">• first_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours	String	No



	<ul style="list-style-type: none">■ d : days■ w : weeks■ m : months		
last_seen_after	<p>< date or epoch or sec or period ></p> <ul style="list-style-type: none">● last_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : month	String	No
last_seen_before	<p>< date or epoch or sec or period ></p> <ul style="list-style-type: none">● last_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period	String	No



	<p>(-36h / -5d / -3w / -6m) - relative time <nX> ago</p> <ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : month		
netmask	<p>Net mask may be given for query types ptr4 or ptr6</p> <ul style="list-style-type: none">● defaults: IPv4 = 32, IPv6 = 128	String	No
regex	<p>re2 regular expression</p> <ul style="list-style-type: none">● pattern must be a valid re2 regular expression	String	No
subdomains	<p>Include or exclude subdomains from qtype a or aaaa results</p> <ul style="list-style-type: none">● 0 = exclude● 1 = include	String	No
Fail on no results	<p>Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.</p>	Checkbox	No

Reverse PADNS Lookup

Capability to do a reverse lookup of Passive DNS data. 7 common parameters are supplied automatically. Enhance your search by adding optional query parameters by referencing: <https://docs.silentpush.com/padns.html#reverse-padns-lookup>.



Configuration Parameters

Table 22

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes
Query Type	The following query types are supported: <ul style="list-style-type: none">• a• aaaa• cname• mx• ns• ptr4• ptr6• soa• txt• mxhash• nshash• soahash• txthash	String	Yes
Query Name	Specify a name or IP address to lookup <ul style="list-style-type: none">• <i>name - wildcards (*)</i> are supported in name string• IPv4• IPv6	String	Yes
first_seen_after	< date or epoch or sec or period > <ul style="list-style-type: none">• first_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format	String	No



	<ul style="list-style-type: none">○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : months		
first_seen_before	<p>< date or epoch or sec or period ></p> <ul style="list-style-type: none">● first_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : months	String	No
last_seen_after	<p>< date or epoch or sec or period ></p> <ul style="list-style-type: none">● last_seen timestamp must be on or after this time	String	No



	<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : month		
last_seen_before	<p>< date or epoch or sec or period ></p> <ul style="list-style-type: none">● last_seen timestamp must be on or after this time<ul style="list-style-type: none">○ date: yyyy-mm-dd (2021-07-09) - fixed date○ epoch: number (1625834953) - fixed time in epoch format○ sec: negative number (-172800) - relative time <sec> seconds ago○ time period: negative number with time period (-36h / -5d / -3w / -6m) - relative time <nX> ago<ul style="list-style-type: none">■ h : hours■ d : days■ w : weeks■ m : month	String	No



netmask	Net mask may be given for query types ptr4 or ptr6 <ul style="list-style-type: none">defaults: IPv4 = 32, IPv6 = 128	String	No
regex	re2 regular expression <ul style="list-style-type: none">pattern must be a valid re2 regular expression	String	No
subdomains	Include or exclude subdomains from qtype a or aaaa results <ul style="list-style-type: none">0 = exclude1 = include	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No

Advanced Request

For other requests that are not included in the premade requests, use this advanced request feature.

For more information on the Silent Push API, please refer to:

<https://docs.silentpush.com/index.html#>

Configuration Parameters

Table 23

Name	Description	Type	Required?
API Key	Silent Push API key	String	Yes



API Endpoint/Path	The API Path request	String	Yes
HTTP Method	HTTP Method to use: Get, POST, DELETE, PUT, HEAD, PATCH, OPTIONS	String	Yes
Query Parameters	Query parameters to append to the URL. For sensitive information like API keys, using variables is recommended to ensure that the Playbook will not export sensitive data.	Key Value	No
Exclude Empty/Null Parameters	Some API endpoint don't handle null/empty query parameters properly (e.g., ?name=&type=String). If selected this options will exclude any query parameters that has a null/empty value.	Checkbox	No
Headers	Headers to include in the request. When using Multi-part Form/File data, do not add a Content-Type header. For sensitive information like API keys, using variables is recommended to ensure that the Playbook will not export sensitive data.	String	No
Fail for status	Fail if the response status code is 4XX - 5XX.	String	No
Fail on no results	Check the box to produce a playbook failure when no results are found. Leave the box unchecked if no failure is required when the response is empty.	Checkbox	No



Frequently Asked Questions (FAQ)

When does the data provided by the Silent Push service begin?

The data starts from 2017.

Why do I not have to add AS or ASN prefix to my ASN value?

The Silent Push API uses the numbers of the ASN only.

What if I get some blank responses?

Please check your Silent Push API key permissions.