

---

# **IronSkillet Documentation**

***Release 1.0.6***

**Scott Shoaf**

**Jan 22, 2020**



---

## Contents:

---

<b>1</b>	<b>IronSkillet Overview</b>	<b>1</b>
<b>2</b>	<b>Requirements and Caveats</b>	<b>5</b>
<b>3</b>	<b>PAN-OS templates</b>	<b>7</b>
<b>4</b>	<b>Panorama templates</b>	<b>19</b>
<b>5</b>	<b>GUI Visual Guide: PAN-OS</b>	<b>33</b>
<b>6</b>	<b>Config Validations: PAN-OS</b>	<b>79</b>
<b>7</b>	<b>Default Loadable Configurations</b>	<b>81</b>
<b>8</b>	<b>Formula-based Excel Spreadsheet</b>	<b>99</b>
<b>9</b>	<b>Creating Loadable Configurations</b>	<b>101</b>
<b>10</b>	<b>Loading the XML templates</b>	<b>105</b>
<b>11</b>	<b>VM-50 Security Profile Limits</b>	<b>115</b>
<b>12</b>	<b>Common or per-device elements</b>	<b>117</b>
<b>13</b>	<b>New PAN-OS Version Updates</b>	<b>119</b>
<b>14</b>	<b>Release and Update History</b>	<b>121</b>



---

## IronSkillet Overview

---

Welcome to the IronSkillet day one configuration templates library.

The next-generation firewall configuration templates are based on existing [best practice recommendations](#) from Palo Alto Networks.

Instead of extensive and detailed ‘how to’ documentation, the templates provide an easy to implement configuration model that is use case agnostic. The emphasis is on key security elements such as dynamic updates, security profiles, rules, and logging that should be consistent across deployments.

### 1.1 Why use day one templates?

Palo Alto Networks has expertise in both security prevention and its own product portfolio. Best practice documentation is designed to provide knowledge sharing of this expertise to customers and partners. This sharing helps improve security posture across various scenarios.

The templates play a complementary role by taking common best practices recommendations and compiling them into pre-built day one configurations that can be readily loaded into Panorama or a next-generation firewall. The benefits include:

- Faster time to implement
- Reduce configuration errors
- Improve security posture

### 1.2 Using the templates

The templates are available on GitHub specific to each PAN-OS software version.

View *github repo*: [ [9.1](#) | [9.0](#) | [8.1](#) | [8.0](#) |  
]

---

**Note:** version 8.0 is still available but no longer will be updated due to sw release EOE

---

Use the branch specific to the software release for your deployment.

The library consists of a set of xml and set configuration templates grouped by:

- `panos` for stand-alone next-gen firewall deployments
- `panorama` for Panorama system and managed device configurations

The templates in each device-type folder include:

- `snippets` for more granular configuration elements
- `full config file` to use for bootstrap or full import + load into a device
- `set commands` for traditional CLI configuration

There are also validation skilletts for analysis of existing configurations

- `full assessment` to see what IronSkillet elements are missing
- `9.x upgrade from 8.1` to check for new skillet additions

Validation insights currently require applications such as panHandler (<https://panhandler.readthedocs.io>) for analysis and results output.

### 1.2.1 Quick start using loadable configurations

The repo contains a set of ready-to-go loadable configurations that use iron-skillet placeholder values. Formats include both xml and set commands.

The xml file can be imported and loaded easily to Panorama or a firewall. The set command model requires 'copy-and-paste' from the CLI.

More information for loading and editing these configurations can be found at: *Default Loadable Configurations*.

### 1.2.2 Excel set command spreadsheet

Also included for easy loading is an Excel formula-based spreadsheet with set commands. A variable value worksheet can be edited to update the spreadsheet using localized values for various configuratino attributes.

More information for using the spreadsheet can be found at: *Formula-based Excel Spreadsheet*.

### 1.2.3 Jinja-based xml snippet and set command templates

Scripting or automation-centric users may prefer to use the base template files. These are variable-based templates using a `jinja {{ variable }}` notation.

The xml snippets with metadata are designed to use API-based configuration loading into Panorama or the firewall and can be coupled with workflow tools for repeatable deployments.

Sample utilities are provided in the `tools` directory to create loadable configurations using these base templates.

See the sections *Creating Loadable Configurations* and *Loading the XML templates* for more information.

---

**Note:** Day one templates are not complete configuration templates. To insert the device into the network requires interface, zone, routing, and other settings outside the scope of the day one templates. Also not included are use-case

specific items such as whitelist security rules, userID settings, and decryption policies that can be deployment and use case specific.

---

## **1.3 What is next after loading a template?**

Based on the deployment scenario, the next steps may include:

- GUI configuration of additional configuration elements specific to the deployment use case
- API/scripted loading of additional configuration elements

In cases where the use case configuration has been merged with the templates, no further actions may be required. A key example would be interface, NAT, zone, and security rule additions for a simple Internet gateway deployments.

## **1.4 Where can I find complete reference use case configurations?**

The initial release of the templates are use case agnostic. However, as the community creates and shared reference configurations, they will be shared across the community as an extension of the iron-skillet configurations.



---

## Requirements and Caveats

---

Please read before using the IronSkillet configuration templates.

### 2.1 Requirements

Using IronSkillet requires the following to properly load into Panorama and/or the NGFW

- Running software version 9.0
  - [Upgrade the firewall to 9.0](#)
  - [Upgrade Panorama to 9.0](#)
- Active subscription for Threat Prevention
  - [Activate the subscription licenses](#)
- Updated application and antivirus content
  - [Install content and software updates](#)

---

**Note:** The links are specific to PAN-OS v9.0 and users may switch to 8.0 or 8.1 based on deployed release

---

---

**Note:** Threat Prevention and the antivirus content update are both required to gain access to the Palo Alto Networks provided External Dynamic Lists (EDLs) used in the security policies.

---

---

**Note:** URL Filtering, DNS Cloud Service, and Wildfire subscriptions are not required to load the configuration but are highly recommended as part of the best practice to utilize IronSkillet elements such as the URL Filtering, Spyware, and Wildfire security profiles and associated profile groups

---

## 2.2 Caveats

Please review the following to understand any limitations or recommendations regarding the IronSkillet templates

- Be sure to edit or the default administrative superuser account if not part of initial configuration
  - If the default account information is used, the user is notified at login
  - To change or add superuser accounts see [Configure a Firewall Administrator](#)
- The current version only supports IPv4 management interface configuration
  - IPv6 to be considered based on customer demand
- IronSkillet loaded into a VM-50 will utilize the full profile capacity
  - See the section *VM-50 Security Profile Limits* for more information
- The Panorama full configuration template is based on a fully shared model
  - All [device-group configuration](#) at the Shared top of tree
  - Additional Panorama [template stacks](#) should include the IronSkillet template

---

## PAN-OS templates

---

The configuration snippet descriptions and the associated GitHub repository link for each xml snippet.

---

**Note:** The template version is found in the template xml file as a tag attribute

---

---

**Note:** The set commands utilize the same configuration settings

---

### 3.1 General Device Configuration

---

This section provides templated configurations for general device settings.

#### 3.1.1 Management Users

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Management configuration superuser access

- Administrative user name
- Password hash stored in the configuration file

#### 3.1.2 Password Complexity

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Administrative user password complexity profile

- Attributes including minimum length, characters, and history

### 3.1.3 Security-related Device Settings

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

General device settings that effect security posture. Found in Device > Setup in the GUI.

- Wildfire: set optimal file size limits for Wildfire uploads and show verdict responses for grayware, malware and phishing
- X-Forwarded-For: To ensure that attackers can't read and exploit the XFF values in web request packets that exit the firewall.
  - Enable the firewall to use XFF values in policies and in the source user fields of logs
  - Remove XFF values from outgoing web requests.
- Session rematch: the firewall will go through all the existing sessions and apply the new security policy to any matching traffic
- Notify User: user should be notified when web-application is blocked; enables the application response page
- Log Suppression: disabled to ensure unique log entries even if similar session types
- Prevent TCP and UDP buffer overflow and multi-part HTTP download evasions
  - Disable 'allow HTTP header range'
  - Disable 'tcp-bypass-exceed-queue'
  - Disable 'udp-bypass-exceed-queue'
- Enable high DP load logging
- Prevent App-ID buffer overflow evasion
  - set bypass-exceed-queue to 'no'
- Prevent TCP and MPTCP evasions
  - set urgent data to 'clear'
  - set drop zero flag to 'yes'
  - set bypass-exceed-oo-queue to 'no'
  - set check-timestamp-option to 'yes'
  - set strip-mptcp-option to yes
- Set an API key lifetime instead of a permanent/static value
  - default set to 525,600 minutes (1 year)
- set export of csv log file to maximum of 1,048,576
- Administrative lockout and access
  - failed attempts and lockout time
  - idle timeout
  - auto acquire commit lock

### 3.1.4 System Configuration

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

*View dns xml snippet:* [ 9.0 | 9.1 ]

*View mgmt IP config xml snippet:* [ 9.0 | 9.1 ]

System configuration settings for dynamic updates and network services (eg. DNS, NTP).

- Update schedule settings
  - Turn on all telemetry settings
  - Check every 30 minutes for new threat signatures
  - Hourly checks for new AV signatures
  - Check every minute for new Wildfire signatures
  - Recommended time delays and thresholds for checks and installs
  - Check for GlobalProtect datafile and clientless vpn updates
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC
- Provide a standard login banner warning for unauthorized users

---

**Note:** The management config types include static or dhcp-client. This is specific to each deployment and can be selected as part of the tools to build `loadable_configs`. Since management interface is in the template config, this option must be included for deployment.

---

## 3.2 Logging

---

Logging best practice configurations for logging output and forwarding profiles.

**Warning: Configure logging profiles before security rules** The template creates a log forwarding profile call default. This profile is referenced in the template security rules and should be configured before the security rules.

---

**Note: Logging can be deployment dependent** The destination in the logging profile is templated to an unroutable syslog server address. This can vary based on actual deployment scenarios.

---

### 3.2.1 Log forwarding profile

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

*View email xml snippet:* [ 9.0 | 9.1 ]

Log forward profile referenced in security rules to determine where to forward log related events.

- Forward all log activity to syslog (see the reference syslog configuration in shared\_log\_settings.xml)
- Email malicious and phishing Wildfire verdicts to the address in the email profile (see shared\_log\_settings.xml)

### 3.2.2 Device log settings

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

*View email profile xml snippet:* [ 9.0 | 9.1 ]

*View email system critical xml snippet:* [ 9.0 | 9.1 ]

Device event logging including sample profiles for email and syslog forwarding.

- Reference syslog profile that can be edited for a specific IP address and UDP/TCP port
- Reference email profile that can be edited for specific email domain and user information
- System, configuration, user, HIP, and correlation log forwarding to syslog
- Email critical system events to the email profile

---

**Note: When to use email alerts** The purpose of select email alert forwarding is ensure not to under alert or over alert yet provide critical messages for key events. Under alerting reduces visibility to key events while over alerting creates too much noise in the system. The templates are set with a median view to capture key events without too much ‘log fatigue’ noise

---

## 3.3 Referenced Objects

---

Address, External Dynamic List (EDL), and tag objects that are referenced in security rules by name.

### 3.3.1 Address Object

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Address object used to reference named addresses.

- **Sinkhole-IPv4:**
  - [8.x] IP address used in security rule to block sinkhole traffic
  - [9.x] FQDN address used in security rule to block sinkhole traffic
- Sinkhole-IPv6: IP address used in security rule to block sinkhole traffic

### 3.3.2 Tags

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.0 ]

Tags used in security rules and related objects.

- Inbound - inbound (untrust to trust) elements
- Outbound - outbound (trust to untrust) elements

- Internal - internal (trust) segmentation elements

## 3.4 Security Profiles and Groups

The key elements for security posture are security profiles and the security rules. The templates ensure best practice profiles and profile groups are available and can be referenced in any security rules. The template security rules focus on ‘top of the list’ block rules to reduce the attack surface.

**Warning: Profiles and subscriptions** All of the template security profiles other than file blocking require Threat Prevention, URL Filtering, and Wildfire subscriptions. Ensure that the device is properly licensed before applying these configurations.

### 3.4.1 Custom URL Category

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Placeholder for custom url categories used in security rules and url profiles. Using these categories prevents the need to modify the default template.

- Black-List: placeholder to be used in block rules and objects to override default template behavior
- White-List: placeholder to be used in permit rules and objects to override default template behavior
- Custom-No-Decrypt: to be used in the decryption no-decrypt rule to specify URLs that should not be decrypted

### 3.4.2 File Blocking

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Security profile for actions specific to file blocking (FB).

**Note: File blocking and file types** The Block file type recommendation is based on common malicious file types with minimal impact in a Day 1 deployment. Although PE is considered the highest risk file type it is also used for legitimate purposes so blocking PE files will be deployment specific and not included in the template.

- Day 1 Block file types: 7z, bat, chm, class, cpl, dll, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf
- The profiles will alert on all other file types for logging purposes

Profiles:

- Outbound-FB: For outbound (trust to untrust) security rules
- Inbound-FB: For inbound (untrust to trust) security rules
- Internal-FB: For internal network segmentation rules
- Alert-Only-FB: No file blocking, only alerts for logging purposes
- Exception-FB: For exception requirements in security rules to avoid modifying the default template profiles

### 3.4.3 Anti-Spyware

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Security profile for actions specific to anti-spyware (AS).

---

**Note: Sinkhole addresses** The profiles use IPv4 and IPv6 addresses for DNS sinkholes. IPv4 is currently provided by Palo Alto Networks. IPv6 is a bogon address. In 9.0 the IPv4 address is replaced by an FQDN

---

[9.0] Support for DNS Cloud subscription service

- In addition to the current malicious domain push to the device, also include domain lookups using the cloud service

Profiles:

- Outbound-AS : For outbound (trust to untrust) security rules
  - Block severity = Critical, High, Medium
  - Default severity = Low, Informational
  - DNS Sinkhole for IPv4 and IPv6
  - Single packet capture for Critical, High, Medium severity
- Inbound-AS : For inbound (untrust to trust) security rules
  - Block severity = Critical, High, Medium
  - Default severity = Low, Informational
  - DNS Sinkhole for IPv4 and IPv6
  - Single packet capture for Critical, High, Medium severity
- Internal-AS : For internal network segmentation rules
  - Block severity = Critical, High
  - Default severity = Medium, Low, Informational
  - DNS Sinkhole for IPv4 and IPv6
  - Single packet capture for Critical, High, Medium severity
- Alert-Only-AS : No blocking, only alerts for logging purposes
  - Alert all severities and malicious domain events
  - No packet capture
- Exception-AS : For exception requirements in security rules to avoid modifying the default template profiles

### 3.4.4 URL Filtering

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Security profile for actions specific to URL filtering (URL).

---

**Note:** Only BLOCK categories will be listed for each profile below. All other URL categories will be set to ALERT in the templates for logging purposes. The complete list of categories can be found in the url filtering template.

---

Profiles:

- Outbound-URL : For outbound (trust to untrust) security rules
  - URL Categories
  - Site Access: Block command-and-control, malware, phishing, hacking, grayware Black List (custom URL category)
  - User Credential Submission: Block all categories
  - Alert category = includes White List (custom URL category)
  - URL Filtering Settings: HTTP Header Logging (user agent, referer, X -Forwarded-For)
- Alert-Only-URL : No blocking, only alerts for logging purposes
  - Alert all categories including custom categories Black List and White List
- Exception-URL : For exception requirements in security rules to avoid modifying the default template profiles
  - URL Categories
  - Site Access: Block command-and-control, malware, phishing, hacking, grayware Black List (custom URL category)
  - User Credential Submission: Block all categories
  - Alert category = includes White List (custom URL category)
  - URL Filtering Settings: HTTP Header Logging (user agent, referer, X -Forwarded-For)

---

**Note:** 9.0 included new URL categories for risk and newly created domains. In future best practices, these categories may be used to provide additional security protections when combined with existing URL categories. For now, these categories are only set to *alert*.

---

### 3.4.5 Anti-Virus

View xml snippet: [ 8.0 | 8.1 | 9.0 | 9.1 ]

Security profile for actions specific to AntiVirus (AV).

Profiles:

- Outbound-AV: For outbound (trust to untrust) security rules
- Inbound-AV: For inbound (untrust to trust) security rules
- Internal-AV: For internal network segmentation rules
- Alert-Only-AV: No blocking, only alerts for logging purposes
- Exception-AV: For exception requirements in security rules to avoid modifying the default template profiles

---

**Note:** Email response codes with SMTP not IMAP or POP3 Reset-both is used for SMTP, IMAP, and POP3. SMTP '541' response messages are returned to notify that the session was blocked. IMAP and POP3 do not have the same response model. In live deployments, instead of DoS concerns with retries, the endpoints typically stop resending after a small number of sends with timeouts.

---

---

**Note:** 9.0 includes support for http/2. If you are upgrading from a previous version ensure that this decoder matches the actions for standard http.

---

### 3.4.6 Vulnerability Protection

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Profiles:

- Outbound-VP : For outbound (trust to untrust) security rules
  - Block severity = Critical, High, Medium
  - Alert severity = Low, Informational
  - Single packet capture for Critical, High, Medium severity
- Inbound-VP : For inbound (untrust to trust) security rules
  - Block severity = Critical, High, Medium
  - Alert severity = Low, Informational
  - Single packet capture for Critical, High, Medium severity
- Internal-VP : For internal network segmentation rules
  - Block severity = Critical, High
  - Alert severity = Medium, Low, Informational
  - Single packet capture for Critical, High, Medium severity
- Alert-Only-VP : No blocking, only alerts for logging purposes
  - Alert all severities
  - No packet capture
- Exception-VP: For exception requirements in security rules to avoid modifying the default template profiles

---

**Note:** A separate branch is being used as a placeholder for [Brute-Force-Exceptions](#). This provides a way to include Support recommended exceptions by ThreatID value. These can be loaded using console SET commands or using API-based tools

---

### 3.4.7 Wildfire Analysis

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Security profile for actions specific to Wildfire upload and analysis (WF).

---

**Note:** `Public Cloud` is the default All template profiles are configured to upload all file types in any direction to the public cloud for analysis.

---

Profiles:

- Outbound-WF: For outbound (trust to untrust) security rules

- Inbound-WF: For inbound (untrust to trust) security rules
- Internal-WF: For internal network segmentation rules
- Alert-Only-WF: No blocking, only alerts for logging purposes
- Exception-WF: For exception requirements in security rules to avoid modifying the default template profiles

### 3.4.8 Security Profile Groups

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Security profile groups based on use case

- Inbound: For rules associated to inbound (untrust to trust) sessions
- Outbound: For rules associated to outbound (trust to untrust) sessions
- Internal: For rules associated to trust-domain network segmentation
- Alert Only: Provides visibility and logging without a blocking posture

## 3.5 Security Rules

---

### 3.5.1 Recommended Block Rules

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Recommended block rules for optimal security posture with associated default log-forwarding profile

- Outbound Block Rule: Block destination IP address match based on the Palo Alto Networks predefined externals dynamic lists
- Inbound Block Rule: Block source IP address match based on the Palo Alto Networks predefined externals dynamic lists
- DNS Sinkhole Block: Block sessions redirected to defined sinkhole addresses using the address objects (address.xml)

---

**Note: Security rules in the template are block only** The template only uses block rules. Allow rules are zone, direction and use case dependent. Additional templating work will provide recommended use case case security rules.

---

### 3.5.2 Default Security Rules

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Configuration for the default interzone and intrazone default rules

- Intrazone
  - Enable logging at session-end using the default logging profile
  - Use the Internal security profile-group
- Interzone

- Explicit drop of traffic between zones
- Enable logging at session-end using the default logging profile

## 3.6 Decryption

---

### 3.6.1 Profiles

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Recommended\_Decryption\_Profile. Referenced by the default decryption rule.

- SSL Forward Proxy
  - Server Cert Verification : Block sessions with expired certs, Block sessions with untrusted issuers, Block sessions with unknown cert status
  - Unsupported Mode Checks : Block sessions with unsupported versions, Blocks sessions with unsupported cipher suites
- SSL No Proxy
  - Server Cert Verification : Block sessions with expired certs, Block sessions with untrusted issuers
- SSH Proxy
  - Unsupported Mode Checks : Block sessions with unsupported versions, Block sessions with unsupported algorithms
- SSL Protocol Settings:
  - Minimum Version: TLSv1.2; Any TLSv1.1 errors can help find outdated TLS endpoints
  - Key Exchange Algorithms: RSA not recommended and unchecked
  - Encryption Algorithms: 3DES and RC4 not recommended and unavailable when TLSv1.2 is the min version
  - Authentication Algorithms:MD5 not recommended and unavailable when TLSv1.2 is the min version

### 3.6.2 Decryption Rules

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Recommended SSL decryption pre-rules for no-decryption.

- NO decrypt rule for select URL categories; Initially disabled in the Day 1 template until SSL decryption to be enabled
- NO decrypt rule used to validate SSL communications based on the `Recommended Decrypt profile`

## 3.7 Zone Protection

---

### 3.7.1 Profile

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Recommended `Zone_Protection` profile for standard, non-volumetric best practices. This profile should be attached to all interfaces within the network.

---

**Note: Recon Protection** Default values enabled in alert-only mode; active blocking posture requires network tuning

---

Packet Based Attack Protection

- IP Drop: Spoofed IP Address, Malformed
- TCP Drop: Remove TCP timestamp, No TCP Fast Open, Multipath TCP (MPTCP) Options = Global

## 3.8 Reports

---

### 3.8.1 Reports

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Series of reports to look for traffic anomalies, where to apply or remove rules, etc. Reports are grouped by topic per the report group section below.

---

**Note: Zones and Subnets in report queries** The repo contains a separate folder for custom reports that use a placeholder zone called 'internet' for match conditions in reports. This value **MUST** be changed to match the actual public zone used in a live network. Additional zones and/or subnets to be used or excluded in the reports would be added in the query values.

---

### 3.8.2 Report Groups

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Template report groups include:

Simple (included in Day One template)

- Possible Compromise: malicious sites and verdicts, sinkhole sessions

Custom

- User Group Activity (eg. Employee, Student, Teacher): user-id centric reports grouped by user type
- Inbound/Outbound/Internal Rule Tuning: Used rules, app ports, unknown apps, geo information
- Inbound/Outbound/Internal Threat Tuning: Allowed threats traversing the device
- File Blocking Tuning: View of upload/download files and types with associated rule
- URL Tuning: Views by categories, especially questionable and unknown categories

- Inbound/Outbound/Internal Threats Blocked: Threat reports specific to blocking posture; complement to threat tuning
- Non-Working Traffic: View of dropped, incomplete, or insufficient data sessions

### 3.8.3 Email Scheduler

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Schedule and email recipients for each report group. The template uses a sample email profile configured in `shared_log_settings`.

---

## Panorama templates

---

The configuration snippet descriptions and the associated GitHub repository link for each xml snippet.

Panorama can be configured using shared elements and device-specific elements. For xml configurations the use of shared or device-specific configurations is based on the xpath location of the snippets. Set commands also denote shared or device-specific configurations. The provided xml snippets have variations in the .meta-cnc.yaml files specifying shared or device-specific placement in the configuration while the set commands and default loadable configuration are shared only.

### Grouping of XML snippets

The xml template directories are group according to the user environment:

- *snippets\_panorama*: A full Panorama configuration using shared device-group and template configurations
- *snippets\_panorama\_dgtemplate\_shared*: used to add shared device-group and baseline template content without Panorama system elements
- *snippets\_panorama\_not\_shared*: a full Panorama configuration with the device-group and stack containing all configuration elements. Nothing is shared.
- *snippets\_panorama\_dgstack\_notshared*: used to add additional device-groups and stack, each with full configuration elements. Nothing is shared.

---

**Note:** The template version is found in the template xml file as a tag attribute

---

---

**Note:** The set commands utilize the same configuration settings

---

## 4.1 General Device Configuration

---

This section provides templated configurations for general device settings.

### 4.1.1 Panorama Admin Users

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Management configuration superuser access

- Administrative user name
- Password hash stored in the configuration file

### 4.1.2 Panorama Password Complexity

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Administrative user password complexity profile

- Attributes including minimum length, characters, and history

### 4.1.3 Panorama settings

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

System configuration settings for dynamic updates and network services (eg. DNS, NTP).

- Update schedule settings
  - Turn on all telemetry settings
  - Check every 30 minutes for new threat signatures
  - Hourly checks for new AV signatures
  - Check every minute for new Wildfire signatures
  - Recommended time delays and thresholds for checks and installs
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC
- Provide a standard login banner warning for unauthorized users

---

**Note:** The Panorama deployment types include ``standard`` or ``cloud`` for AWS, Azure, or GCP environments. This is an option in the tools ``build_my_config`` utility to use the proper config option in the template.

---

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Panorama management settings

- Set 'enable reporting on groups' to 'yes'
- Disable sharing unused objects with devices
- Set an API key lifetime instead of a permanent/static value
  - default set to 525,600 minutes (1 year)
- set export of csv log file to maximum of 1,048,576
- Administrative lockout and access

- failed attempts and lockout time
- idle timeout
- auto acquire commit lock

#### 4.1.4 Security-related Device Settings

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

General device settings that effect security posture. Found in Device > Setup in the GUI.

- Wildfire: set optimal file size limits for Wildfire uploads and show verdict responses for grayware, malware and phishing
- X-Forwarded-For: To ensure that attackers can't read and exploit the XFF values in web request packets that exit the firewall.
  - Enable the firewall to use XFF values in policies and in the source user fields of logs
  - Remove XFF values from outgoing web requests.
- Session rematch: the firewall will go through all the existing sessions and apply the new security policy to any matching traffic
- Notify User: user should be notified when web-application is blocked; enables the application response page
- Log Suppression: disabled to ensure unique log entries even if similar session types
- Prevent TCP and UDP buffer overflow and multi-part HTTP download evasions
  - Disable 'allow HTTP header range'
  - Disable 'tcp-bypass-exceed-queue'
  - Disable 'udp-bypass-exceed-queue'
- Enable high DP load logging
- Prevent App-ID buffer overflow evasion
  - set bypass-exceed-queue to 'no'
- Prevent TCP and MPTCP evasions
  - set urgent data to 'clear'
  - set drop zero flag to 'yes'
  - set bypass-exceed-oo-queue to 'no'
  - set check-timestamp-option to 'yes'
  - set strip-mptcp-option to yes
- Set an API key lifetime instead of a permanent/static value
  - default set to 525,600 minutes (1 year)
- set export of csv log file to maximum of 1,048,576

## 4.1.5 System Configuration

View xml snippet: [ 8.0 | 8.1 | 9.0 | 9.1 ]

System configuration settings for dynamic updates and network services (eg. DNS, NTP).

- Update schedule settings
  - Turn on all telemetry settings
  - Check every 30 minutes for new threat signatures
  - Hourly checks for new AV signatures
  - Check every minute for new Wildfire signatures
  - Recommended time delays and thresholds for checks and installs
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC
- Provide a standard login banner warning for unauthorized users

---

**Note:** The management config types include static or dhcp-client. This is specific to each deployment and can be selected as part of the tools to build `loadable_configs`. Since management interface is in the template config, this option must be included for deployment.

---

## 4.2 Logging

---

Logging best practice configurations for logging output and forwarding profiles. Also Panorama-specific settings for Panorama as a log collector

**Warning:** Configure logging profiles before security rules The template creates a log forwarding profile call default. This profile is referenced in the template security rules and should be configured before the security rules.

---

**Note:** **Logging can be deployment dependent** The destination in the logging profile is templated to an unroutable syslog server address. This can vary based on actual deployment scenarios.

---

### 4.2.1 Log forwarding profile

View xml snippet: [ 8.0 | 8.1 | 9.0 | 9.1 ]

Log forward profile referenced in security rules to determine where to forward log related events.

- Forward all log activity to Panorama (see the reference syslog configuration in `shared_log_settings.xml`)
- Email malicious and phishing Wildfire verdicts to the address in the email profile (see `shared_log_settings.xml`)

### 4.2.2 Device log settings

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Device event logging including sample profiles for email and syslog forwarding.

- Reference syslog profile that can be edited for a specific IP address and UDP/TCP port
- Reference email profile that can be edited for specific email domain and user information
- System, configuration, user, HIP, and correlation log forwarding to syslog
- Email critical system events to the email profile

---

**Note: When to use email alerts** The purpose of select email alert forwarding is ensure not to under alert or over alert yet provide critical messages for key events. Under alerting reduces visibility to key events while over alerting creates too much noise in the system. The templates are set with a median view to capture key events without too much 'log fatigue' noise

---

### 4.2.3 Panorama log settings

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Panorama event logging including sample profiles for email and syslog forwarding.

- Reference syslog profile that can be edited for a specific IP address and UDP/TCP port
- Reference email profile that can be edited for specific email domain and user information
- System, configuration, user, HIP, and correlation log forwarding to Panorama
- Traffic and threat related log configuration forwarding to Panorama

### 4.2.4 Panorama log collector group

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

After you configure Log Collectors and firewalls, you must assign them to a Collector Group so that the firewalls can send logs to the Log Collectors.

This is a placeholder default log collector group providing proper log forwarding and real-time email alerting configuration. In many cases deployments under-alert or over-alert real time losing visibility to something drastic because it is never sent to lost in then noise of too many emails.

- Syslog all logs using the sample syslog profile
- Email alerts for critical system logs and Wildfire malware/phishing verdicts that require immediate attention

## 4.3 Referenced Objects

---

Address, External Dynamic List (EDL), and tag objects that are referenced in security rules by name.

### 4.3.1 Address Object

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Address object used to reference named addresses.

- **Sinkhole-IPv4:**
  - [8.x] IP address used in security rule to block sinkhole traffic
  - [9.0] FQDN address used in security rule to block sinkhole traffic
- Sinkhole-IPv6: IP address used in security rule to block sinkhole traffic

### 4.3.2 Tags

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Tags used in security rules and related objects.

- Inbound - inbound (untrust to trust) elements
- Outbound - outbound (trust to untrust) elements
- Internal - internal (trust) segmentation elements

## 4.4 Security Profiles and Groups

---

The key elements for security posture are security profiles and the security rules. The templates ensure best practice profiles and profile groups are available and can be referenced in any security rules. The template security rules focus on 'top of the list' block rules to reduce the attack surface.

**Warning: Profiles and subscriptions** All of the template security profiles other than file blocking require Threat Prevention, URL Filtering, and Wildfire subscriptions. Ensure that the device is properly licensed before applying these configurations.

### 4.4.1 Custom URL Category

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Placeholder for custom url categories used in security rules and url profiles. Using these categories prevents the need to modify the default template.

- Black-List: placeholder to be used in block rules and objects to override default template behavior
- White-List: placeholder to be used in permit rules and objects to override default template behavior
- Custom-No-Decrypt: to be used in the decryption no-decrypt rule to specify URLs that should not be decrypted

## 4.4.2 File Blocking

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Security profile for actions specific to file blocking (FB).

---

**Note: File blocking and file types** The Block file type recommendation is based on common malicious file types with minimal impact in a Day 1 deployment. Although PE is considered the highest risk file type it is also used for legitimate purposes so blocking PE files will be deployment specific and not included in the template.

- Day 1 Block file types: 7z, bat, chm, class, cpl, dll, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf
  - The profiles will alert on all other file types for logging purposes
- 

Profiles:

- Outbound-FB: For outbound (trust to untrust) security rules
- Inbound-FB: For inbound (untrust to trust) security rules
- Internal-FB: For internal network segmentation rules
- Alert-Only-FB: No file blocking, only alerts for logging purposes
- Exception-FB: For exception requirements in security rules to avoid modifying the default template profiles

## 4.4.3 Anti-Spyware

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Security profile for actions specific to anti-spyware (AS).

---

**Note: Sinkhole addresses** The profiles use IPv4 and IPv6 addresses for DNS sinkholes. IPv4 is currently provided by Palo Alto Networks. IPv6 is a bogon address. In 9.0 the IPv4 address is replaced by an FQDN

---

[9.x] Support for DNS Cloud subscription service

- In addition to the current malicious domain push to the device, also include domain lookups using the cloud service

Profiles:

- Outbound-AS : For outbound (trust to untrust) security rules
  - Block severity = Critical, High, Medium
  - Default severity = Low, Informational
  - DNS Sinkhole for IPv4 and IPv6
  - Single packet capture for Critical, High, Medium severity
- Inbound-AS : For inbound (untrust to trust) security rules
  - Block severity = Critical, High, Medium
  - Default severity = Low, Informational
  - DNS Sinkhole for IPv4 and IPv6
  - Single packet capture for Critical, High, Medium severity

- Internal-AS : For internal network segmentation rules
  - Block severity = Critical, High
  - Default severity = Medium, Low, Informational
  - DNS Sinkhole for IPv4 and IPv6
  - Single packet capture for Critical, High, Medium severity
- Alert-Only-AS : No blocking, only alerts for logging purposes
  - Alert all severities and malicious domain events
  - No packet capture
- Exception-AS : For exception requirements in security rules to avoid modifying the default template profiles

#### 4.4.4 URL Filtering

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Security profile for actions specific to URL filtering (URL).

---

**Note:** Only BLOCK categories will be listed for each profile below. All other URL categories will be set to ALERT in the templates for logging purposes. The complete list of categories can be found in the url filtering template.

---

Profiles:

- Outbound-URL : For outbound (trust to untrust) security rules
  - URL Categories
  - Site Access: Block command-and-control, malware, phishing, hacking, Black List (custom URL category)
  - User Credential Submission: Block all categories
  - Alert category = includes White List (custom URL category)
  - URL Filtering Settings: HTTP Header Logging (user agent, referer, X -Forwarded-For)
- Alert-Only-URL : No blocking, only alerts for logging purposes
  - Alert all categories including custom categories Black List and White List
- Exception-URL : For exception requirements in security rules to avoid modifying the default template profiles
  - URL Categories
  - Site Access: Block command-and-control, malware, phishing, hacking, Black List (custom URL category)
  - User Credential Submission: Block all categories
  - Alert category = includes White List (custom URL category)
  - URL Filtering Settings: HTTP Header Logging (user agent, referer, X -Forwarded-For)

---

**Note:** 9.0 includes new URL categories for risk and newly created domains. In future best practices, these categories may be used to provide additional security protections when combined with existing URL categories. For now, these categories are only set to *alert*.

---

### 4.4.5 Anti-Virus

View xml snippet: [ 8.0 | 8.1 | 9.0 | 9.1 ]

Security profile for actions specific to AntiVirus (AV).

Profiles:

- Outbound-AV: For outbound (trust to untrust) security rules
- Inbound-AV: For inbound (untrust to trust) security rules
- Internal-AV: For internal network segmentation rules
- Alert-Only-AV: No blocking, only alerts for logging purposes
- Exception-AV: For exception requirements in security rules to avoid modifying the default template profiles

---

**Note:** **Email response codes with SMTP not IMAP or POP3** Reset-both is used for SMTP, IMAP, and POP3. SMTP '541' response messages are returned to notify that the session was blocked. IMAP and POP3 do not have the same response model. In live deployments, instead of DoS concerns with retries, the endpoints typically stop resending after a small number of sends with timeouts.

---



---

**Note:** 9.0 includes support for http/2. If you are upgrading from a previous version ensure that this decoder matches the actions for standard http.

---

### 4.4.6 Vulnerability Protection

View xml snippet: [ 8.0 | 8.1 | 9.0 | 9.1 ]

Profiles:

- Outbound-VP : For outbound (trust to untrust) security rules
  - Block severity = Critical, High, Medium
  - Alert severity = Low, Informational
  - Single packet capture for Critical, High, Medium severity
- Inbound-VP : For inbound (untrust to trust) security rules
  - Block severity = Critical, High, Medium
  - Alert severity = Low, Informational
  - Single packet capture for Critical, High, Medium severity
- Internal-VP : For internal network segmentation rules
  - Block severity = Critical, High
  - Alert severity = Medium, Low, Informational
  - Single packet capture for Critical, High, Medium severity
- Alert-Only-VP : No blocking, only alerts for logging purposes
  - Alert all severities
  - No packet capture

- Exception-VP: For exception requirements in security rules to avoid modifying the default template profiles

---

**Note:** A separate branch is being used as a placeholder for [Brute-Force-Exceptions](#). This provides a way to include Support recommended exceptions by ThreatID value. These can be loaded using console SET commands or using API-based tools

---

#### 4.4.7 Wildfire Analysis

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Security profile for actions specific to Wildfire upload and analysis (WF).

---

**Note:** `Public Cloud` is the default All template profiles are configured to upload all file types in any direction to the public cloud for analysis.

---

Profiles:

- Outbound-WF: For outbound (trust to untrust) security rules
- Inbound-WF: For inbound (untrust to trust) security rules
- Internal-WF: For internal network segmentation rules
- Alert-Only-WF: No blocking, only alerts for logging purposes
- Exception-WF: For exception requirements in security rules to avoid modifying the default template profiles

#### 4.4.8 Security Profile Groups

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Security profile groups based on use case

- Inbound: For rules associated to inbound (untrust to trust) sessions
- Outbound: For rules associated to outbound (trust to untrust) sessions
- Internal: For rules associated to trust-domain network segmentation
- Alert Only: Provides visibility and logging without a blocking posture

### 4.5 Security Rules

---

#### 4.5.1 Recommended Block Rules

*View xml snippet:* [ [8.0](#) | [8.1](#) | [9.0](#) | [9.1](#) ]

Recommended block rules for optimal security posture with associated default log-forwarding profile

- Outbound Block Rule: Block destination IP address match based on the Palo Alto Networks predefined externals dynamic lists

- Inbound Block Rule: Block source IP address match based on the Palo Alto Networks predefined external dynamic lists
- DNS Sinkhole Block: Block sessions redirected to defined sinkhole addresses using the address objects (address.xml)

---

**Note: Security rules in the template are block only** The template only uses block rules. Allow rules are zone, direction and use case dependent. Additional templating work will provide recommended use case security rules.

---

## 4.5.2 Default Security Rules

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Configuration for the default interzone and intrazone default rules

- Intrazone
  - Enable logging at session-end using the default logging profile
  - Use the Internal security profile-group
- Interzone
  - Explicit drop of traffic between zones
  - Enable logging at session-end using the default logging profile

## 4.6 Decryption

---

### 4.6.1 Profiles

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Recommended\_Decryption\_Profile. Referenced by the default decryption rule.

- SSL Forward Proxy
  - Server Cert Verification : Block sessions with expired certs, Block sessions with untrusted issuers, Block sessions with unknown cert status
  - Unsupported Mode Checks : Block sessions with unsupported versions, Blocks sessions with unsupported cipher suites
- SSL No Proxy
  - Server Cert Verification : Block sessions with expired certs, Block sessions with untrusted issuers
- SSH Proxy
  - Unsupported Mode Checks : Block sessions with unsupported versions, Block sessions with unsupported algorithms
- SSL Protocol Settings:
  - Minimum Version: TLSv1.2; Any TLSv1.1 errors can help find outdated TLS endpoints
  - Key Exchange Algorithms: RSA not recommended and unchecked

- Encryption Algorithms: 3DES and RC4 not recommended and unavailable when TLSv1.2 is the min version
- Authentication Algorithms: MD5 not recommended and unavailable when TLSv1.2 is the min version

## 4.6.2 Decryption Rules

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Recommended SSL decryption pre-rules for no-decryption.

- NO decrypt rule for select URL categories; Initially disabled in the Day 1 template until SSL decryption to be enabled

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Recommended SSL decryption post-rules for no-decryption.

- NO decrypt rule used to validate SSL communications based on the Recommended Decrypt profile

## 4.7 Zone Protection

---

### 4.7.1 Profile

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Recommended\_Zone\_Protection profile for standard, non-volumetric best practices. This profile should be attached to all interfaces within the network.

---

**Note: Recon Protection** Default values enabled in alert-only mode; active blocking posture requires network tuning

---

Packet Based Attack Protection

- IP Drop: Spoofed IP Address, Malformed
- TCP Drop: Remove TCP timestamp, No TCP Fast Open, Multipath TCP (MPTCP) Options = Global

## 4.8 Reports

---

### 4.8.1 Reports

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Series of reports to look for traffic anomalies, where to apply or remove rules, etc. Reports are grouped by topic per the report group section below.

---

**Note: Zones and Subnets in report queries** The repo contains a separate folder for custom reports that use a placeholder zone called 'internet' for match conditions in reports. This value MUST be changed to match the actual

---

public zone used in a live network. Additional zones and/or subnets to be used or excluded in the reports would be added in the query values.

---

**Note:** To generate reports that include PA-7000 Series log data not forwarding to Panorama, use Remote Device Data as the Data Source. This is only viewable from the `All` device group option and not a specific device group.

---

## 4.8.2 Report Groups

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Template report groups include:

Simple (included in Day One template)

- Possible Compromise: malicious sites and verdicts, sinkhole sessions

Custom

- User Group Activity (eg. Employee, Student, Teacher): user-id centric reports grouped by user type
- Inbound/Outbound/Internal Rule Tuning: Used rules, app ports, unknown apps, geo information
- Inbound/Outbound/Internal Threat Tuning: Allowed threats traversing the device
- File Blocking Tuning: View of upload/download files and types with associated rule
- URL Tuning: Views by categories, especially questionable and unknown categories
- Inbound/Outbound/Internal Threats Blocked: Threat reports specific to blocking posture; complement to threat tuning
- Non-Working Traffic: View of dropped, incomplete, or insufficient data sessions

## 4.8.3 Email Scheduler

*View xml snippet:* [ 8.0 | 8.1 | 9.0 | 9.1 ]

Schedule and email recipients for each report group. The template uses a sample email profile configured in `shared_log_settings`.



---

## GUI Visual Guide: PAN-OS

---

IronSkillet is delivered as a configuration template without a step-by-step configuration guide. This was the intent to have a rapid deployment option without massive GUI clicks.

However, users still want to know what exactly they configured in the event they want to make changes or compare IronSkillet manually to their existing configuration.

So based on popular demand here is the GUI-based visual guide to all of the IronSkillet configuration elements.

This is based on PAN-OS 9.x with callouts for any features not supported in the 8.x releases. Also note that based on software release, there may be other items configured or ‘checked’ as defaults and not part of IronSkillet. These items are not referenced in this guide.

IronSkillet includes a mix of day one best practices for configuration types such as:

- **Device management hardening:** general operations of the NGFW
- **Security traffic hardening:** control of traffic flows that impacts device monitoring
- **Logging and alerts:** data collection and external notifications
- **Security objects and policies:** policy-related config settings and dynamic updates
- **Decryption objects and policies:** certification checks and sample no-decrypt policy

This visual guide is based on the [IronSkillet full configuration file](#)

This file uses default value settings and can be readily imported and loaded as a candidate configuration allowing the user to follow along with this guide.

---

**Note:** Documentation links for release 9.0 are provided for additional information.

---

### 5.1 Device

The device tab is used for device management, hardening, system logging, and other device related configuration elements.

It also includes security function related configuration such as dynamic updates for anti-virus, vulnerability, spyware DNS and Wildfire signatures as well as Wildfire submission file size configuration.

## 5.1.1 Setup

### Management

---

#### See also

General configuration information in the Admin Guide: [Device - Setup - Management](#)

---

#### Device > Setup > Management > General Settings




The screenshot shows the 'General Settings' configuration page. The page has a dark header bar with the title 'General Settings' and a gear icon. The settings are organized into a list of fields and checkboxes. The 'Hostname' is set to 'sample'. The 'Domain' field is empty. The 'Login Banner' contains the text: 'You have accessed a protected system. Log off immediately if you are not an authorized user.' The 'Force Admins to Acknowledge Login Banner' checkbox is unchecked. The 'SSL/TLS Service Profile' is set to 'UTC'. The 'Time Zone' is set to 'UTC'. The 'Locale' is set to 'en'. The 'Time' is set to 'Tue Oct 08 12:22:47 UTC 2019'. The 'Geo Location' is set to 'UTC'. The 'Automatically Acquire Commit Lock' checkbox is checked. The 'Certificate Expiration Check' checkbox is unchecked. The 'Use Hypervisor Assigned MAC Addresses' checkbox is unchecked. The 'GTP Security' checkbox is unchecked. The 'SCTP Security' checkbox is unchecked.

Hostname	sample
Domain	
Login Banner	You have accessed a protected system. Log off immediately if you are not an authorized user.
Force Admins to Acknowledge Login Banner	<input type="checkbox"/>
SSL/TLS Service Profile	UTC
Time Zone	UTC
Locale	en
Time	Tue Oct 08 12:22:47 UTC 2019
Geo Location	UTC
Automatically Acquire Commit Lock	<input checked="" type="checkbox"/>
Certificate Expiration Check	<input type="checkbox"/>
Use Hypervisor Assigned MAC Addresses	<input type="checkbox"/>
GTP Security	<input type="checkbox"/>
SCTP Security	<input type="checkbox"/>

Changes to General Settings:

- **Hostname:** name of the device; IronSkillet defaults to 'sample'
- **Login Banner:** display text presented to users at login
- **Time Zone:** set to UTC so all devices map to a common universal timezone
- **Automatically Acquire Commit Lock:** block a commit across multiple web sessions


**Device > Setup > Management > Authentication Settings**

Authentication Settings 	
Authentication Profile	
Certificate Profile	
Idle Timeout (min)	10
API Key Lifetime (min)	525600
API Keys Last Expired	
Failed Attempts	5
Lockout Time (min)	30

Changes to Authentication Settings:

- **Idle Timeout:** close the session after 10 minutes of inactivity
- **API Key Lifetime (9.0):** time to expire an existing API key; 'infinite' pre 9.0
- **Failed Attempts:** Lockout the account after 5 failed attempts
- **Lockout Time:** Lockout the account for 30 minutes after 5 failed attempts

**Device > Setup > Management > Logging and Reporting Settings**

Logging and Reporting Settings 	
Log Storage	Total: 15.72 GB Unallocated: 120.73 MB
Number of Versions for Config Audit	100
Max Rows in CSV Export	1048576
Max Rows in User Activity Report	5000
Average Browse Time (sec)	60
Page Load Threshold (sec)	20
Send HOSTNAME in Syslog	FQDN
Report Runtime	02:00
Report Expiration Period (days)	
Stop Traffic when LogDb Full	<input type="checkbox"/>
Enable Threat Vault Access	<input checked="" type="checkbox"/>
Enable Log on High DP Load	<input checked="" type="checkbox"/>
Support UTF-8 For Log Output	<input type="checkbox"/>
Log Collector Status	<a href="#">Show Status</a>

Changes to Logging and Reporting Settings:

- **Max Rows in CSV Export:** increase row count to 1,048,576
- **Enable Log on High DP Load:** a system log entry is generated when the packet processing load on the firewall is at 100% CPU utilization

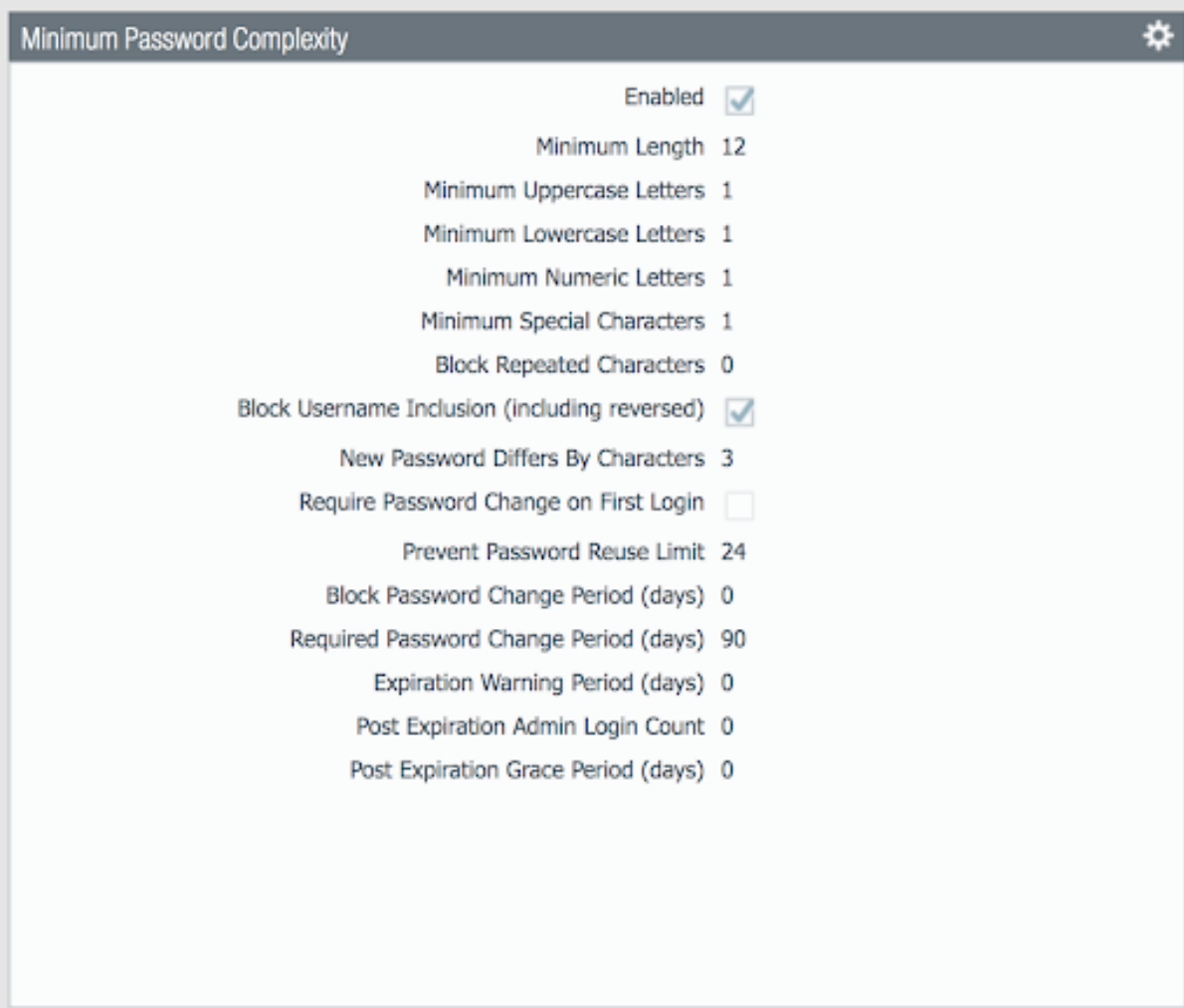
## Log Suppression (CLI only)

Log suppression, when enabled, is a feature that instructs the Palo Alto Networks device to combine multiple similar logs into a single log entry on the Monitor > Logs > Traffic page.

Disabled to ensure unique log entries even if similar session types

```
set deviceconfig setting logging log-suppression no
```

## Device > Setup > Management > Minimum Password Complexity



The screenshot shows the 'Minimum Password Complexity' configuration page. The page has a title bar with the text 'Minimum Password Complexity' and a gear icon. The configuration is as follows:

Setting	Value
Enabled	<input checked="" type="checkbox"/>
Minimum Length	12
Minimum Uppercase Letters	1
Minimum Lowercase Letters	1
Minimum Numeric Letters	1
Minimum Special Characters	1
Block Repeated Characters	0
Block Username Inclusion (including reversed)	<input checked="" type="checkbox"/>
New Password Differs By Characters	3
Require Password Change on First Login	<input type="checkbox"/>
Prevent Password Reuse Limit	24
Block Password Change Period (days)	0
Required Password Change Period (days)	90
Expiration Warning Period (days)	0
Post Expiration Admin Login Count	0
Post Expiration Grace Period (days)	0

Enable minimum password requirements for local accounts. With this feature, you can ensure that local administrator accounts on the firewall will adhere to a defined set of password requirements.

---

**Note:** password expiration has been removed based on NIST standards although users can still opt to set an expiration and notification period

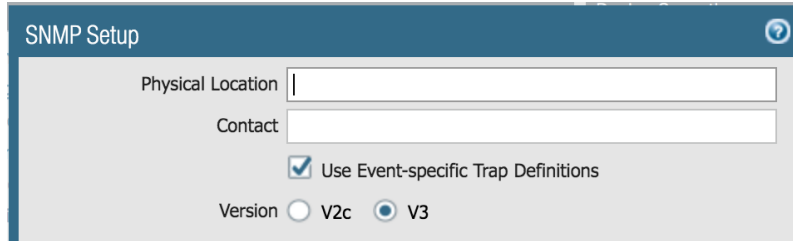
---

## Operations

### See also

General configuration information in the Admin Guide: [Device - Setup - Operations](#)

### Device > Setup > Operations > SNMP Setup



The image shows the 'SNMP Setup' configuration window. It has a title bar with a question mark icon. Inside, there are two text input fields: 'Physical Location' and 'Contact'. Below these is a checkbox labeled 'Use Event-specific Trap Definitions' which is checked. At the bottom, there is a 'Version' section with two radio buttons: 'V2c' and 'V3'. The 'V3' radio button is selected.

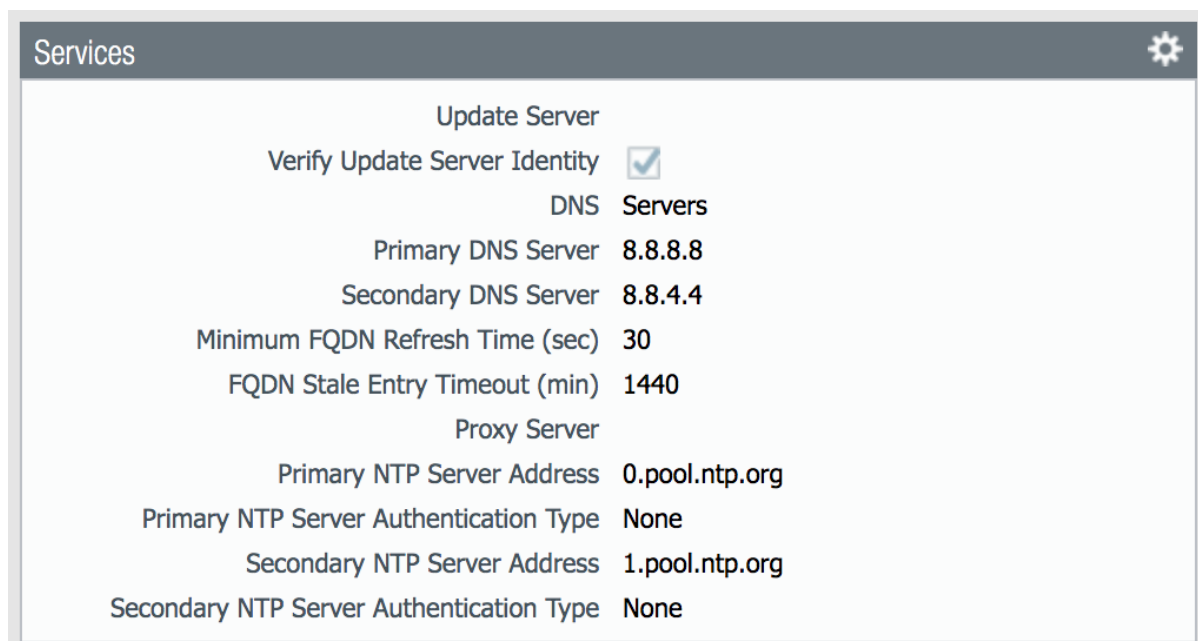
If used, ensure SNMP version is V3

## Services

### See also

General configuration information in the Admin Guide: [Device - Setup - Services](#)

### Device > Setup > Services > Services



The image shows the 'Services' configuration window. It has a title bar with a gear icon. The window contains several configuration sections:

- Update Server**
  - Verify Update Server Identity: ☒
- DNS Servers**
  - Primary DNS Server: 8.8.8.8
  - Secondary DNS Server: 8.8.4.4
  - Minimum FQDN Refresh Time (sec): 30
  - FQDN Stale Entry Timeout (min): 1440
- Proxy Server**
  - Primary NTP Server Address: 0.pool.ntp.org
  - Primary NTP Server Authentication Type: None
  - Secondary NTP Server Address: 1.pool.ntp.org
  - Secondary NTP Server Authentication Type: None

Key configuration elements:

- **DNS:** Primary and Secondary server IP addresses; for all DNS queries that the firewall initiates in support of FQDN address objects, logging, and firewall management
- **NTP:** Primary and Secondary server FQDNs; use to synchronize the clock on the firewall

## Interfaces

---

### See also

General configuration information in the Admin Guide: [Device - Setup - Interfaces](#)

---

### Device > Setup > Interfaces > Management



**Management Interface Settings**

IP Type ☒ Static ☐ DHCP Client

IP Address

Netmask

Default Gateway

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed

MTU

**Administrative Management Services**

☐ HTTP ☒ HTTPS

☐ Telnet ☒ SSH

**Network Services**

☐ HTTP OCSP ☒ Ping

☐ SNMP ☐ User-ID

☐ User-ID Syslog Listener-SSL ☐ User-ID Syslog Listener-UDP

This example shows a static IP address, netmask, and gateway configuration. IronSkillet also gives the option of using the DHCP Client which removes the IP data fields.

- **Administrative Management Services:** limit to HTTPS and SSH
- **Network Services:** only allow Ping unless other services are required

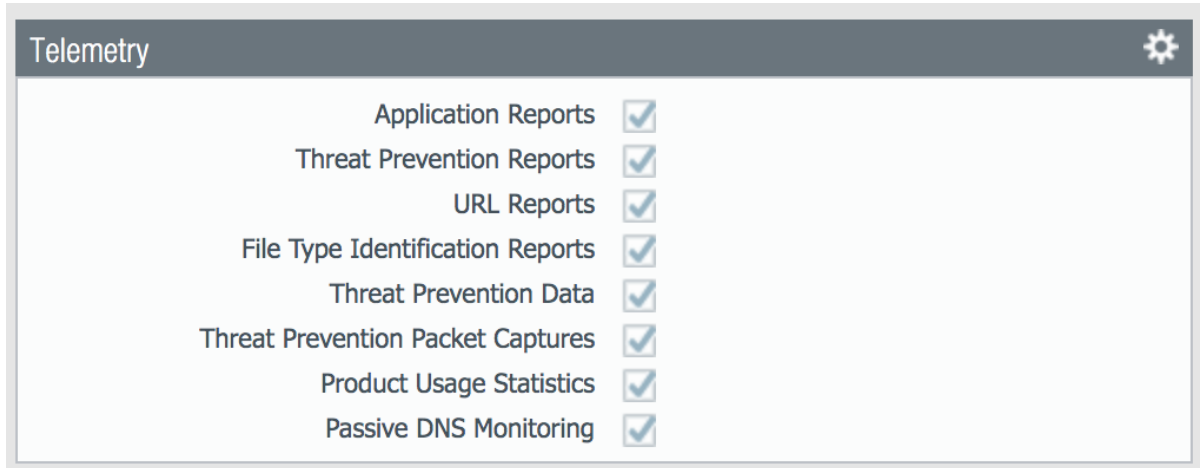
## Telemetry

---

**See also**

General configuration information in the Admin Guide: [Device - Setup - Telemetry](#)

---

**Device > Setup > Telemetry > Telemetry**

IronSkillet sets all telemetry options to enabled.

Telemetry is the process of collecting and transmitting data for analysis. When you enable telemetry on the firewall, the firewall collects and forwards data that includes information on applications, threats, device health, and passive DNS to Palo Alto Networks. All Palo Alto Networks users benefit from the data that each telemetry participant shares, making telemetry a community-driven approach to threat prevention.

Telemetry is an opt-in feature and, for most telemetry data, you can preview the information that the firewall collects. Palo Alto Networks does not share your telemetry data with other customers or third-party organizations.

**Content-ID**

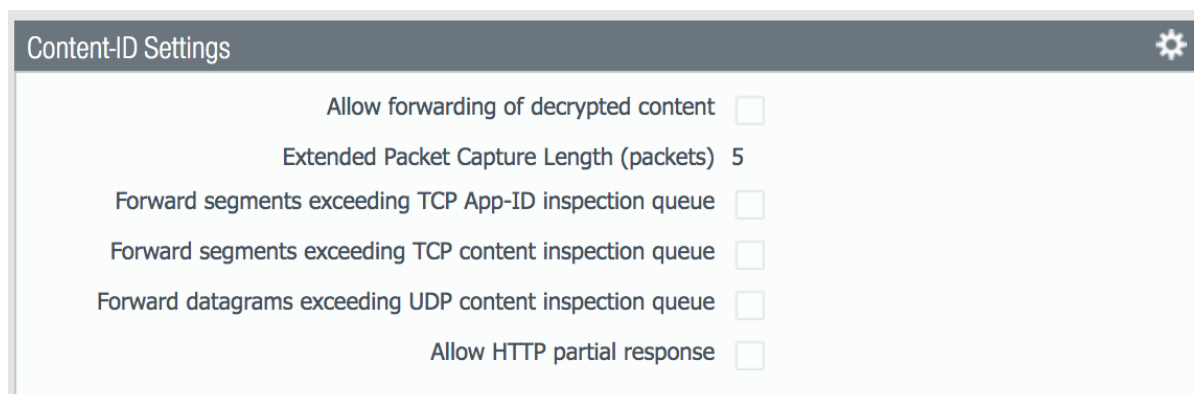
---

**See also**

General configuration information in the Admin Guide: [Device - Setup - Content-ID](#)

---

## Device &gt; Setup &gt; Content-ID &gt; Content-ID Settings



Content-ID Settings

Allow forwarding of decrypted content ☐

Extended Packet Capture Length (packets) 5

Forward segments exceeding TCP App-ID inspection queue ☐

Forward segments exceeding TCP content inspection queue ☐

Forward datagrams exceeding UDP content inspection queue ☐

Allow HTTP partial response ☐

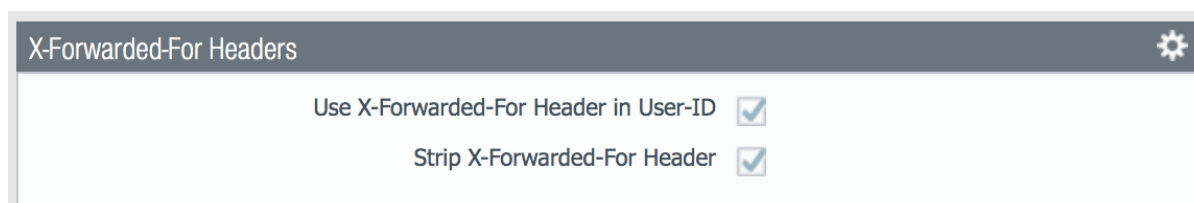
**Disable Forward segments exceeding TCP App-ID inspection queue:** In newer releases disabled by default; explicit disable in IronSkillet template. Disable this option to prevent the firewall from forwarding TCP segments and skipping App-ID inspection when the App-ID inspection queue is full.

**Disable Forward segments exceeding TCP content inspection queue:** Disable this option to prevent the firewall from forwarding TCP segments and skipping content inspection when the content inspection queue is full.

**Disable Forward segments exceeding UDP content inspection queue:** Disable this option to prevent the firewall from forwarding UDP segments and skipping content inspection when the content inspection queue is full.

**Disable Allow HTTP partial response** This option allows a client to fetch only part of a file. When a next-generation firewall in the path of a transfer identifies and drops a malicious file, it terminates the TCP session with an RST packet. If the web browser implements the HTTP Range option, it can start a new session to fetch only the remaining part of the file. This prevents the firewall from triggering the same signature again due to the lack of context into the initial session, while at the same time allowing the web browser to reassemble the file and deliver the malicious content. To prevent this, make sure this option is disabled.

## Device &gt; Setup &gt; Content-ID &gt; X-Forwarded-For Headers



X-Forwarded-For Headers

Use X-Forwarded-For Header in User-ID ☒

Strip X-Forwarded-For Header ☒

Header field option that preserves the IP address of the user who made the GET request

**Enable Use X-Forwarded-For Header in User-ID**

Select this option to specify that User-ID reads IP addresses from the X-Forwarded-For (XFF) header in client requests for web services when the firewall is deployed between the Internet and a proxy server that would otherwise hide client IP addresses. User-ID matches the IP addresses it reads with usernames that your policies reference so that those policies can control and log access for the associated users and groups. If the header has multiple IP addresses, User-ID uses the first entry from the left.

**Enable Strip X-Forwarded-For Header**

Select this option to remove the X-Forwarded-For (XFF) header, which contains the IP address of a client requesting a web service when the firewall is deployed between the Internet and a proxy server. The firewall zeroes out the header value before forwarding the request: the forwarded packets don't contain internal source IP information.

## Wildfire

### See also

General configuration information in the Admin Guide: [Device - Setup - Wildfire](#)

### Device > Setup > Wildfire > General Settings

General Settings	
WildFire Public Cloud	wildfire.paloaltonetworks.com
WildFire Private Cloud	
Use Proxy Settings for Private Cloud	<input type="checkbox"/>
File Size Limits	pe: 10 MB apk: 30 MB pdf: 1000 KB ms-office: 2000 KB jar: 5 MB flash: 5 MB MacOSX: 1 MB archive: 10 MB linux: 2 MB script: 2000 KB
Report Benign Files	<input checked="" type="checkbox"/>
Report Grayware Files	<input checked="" type="checkbox"/>

Key configuration elements:

- **WildFire Public Cloud:** where to send file samples for analysis; defaults to the US-based url and can be changed to various regional sites
- **File Size Limits:** recommended maximum file sizes to send to WildFire
- **Report Benign/Grayware Files:** shows these verdicts in the Wildfire submissions logs

### See also

The [wildfire global cloud documentation](#) has additional information for public cloud fqdn options

## Session

Configure session age-out times, decryption certificate settings, and global session-related settings such as firewalling IPv6 traffic and rematching Security policy to existing sessions when the policy changes.

---

**See also**

General configuration information in the Admin Guide: [Device - Setup - Session](#)

---

**Device > Setup > Session > Session Settings**

Session Settings

Rematch Sessions

☒

ICMPv6 Token Bucket Size

100

ICMPv6 Error Packet Rate (per sec)

100

IPv6 Firewalling

☒

Enable Jumbo Frame

☐

Global MTU

1500

NAT64 IPv6 Minimum Network MTU

1280

NAT Oversubscription Rate

Platform Default

ICMP Unreachable Packet Rate (per sec)

200

Accelerated Aging

☒

Accelerated Aging Threshold

80

Accelerated Aging Scaling Factor

2

Packet Buffer Protection

☐

Alert (%)

50

Activate (%)

50

Block Hold Time (sec)

60

Block Duration (sec)

3600

Multicast Route Setup Buffering

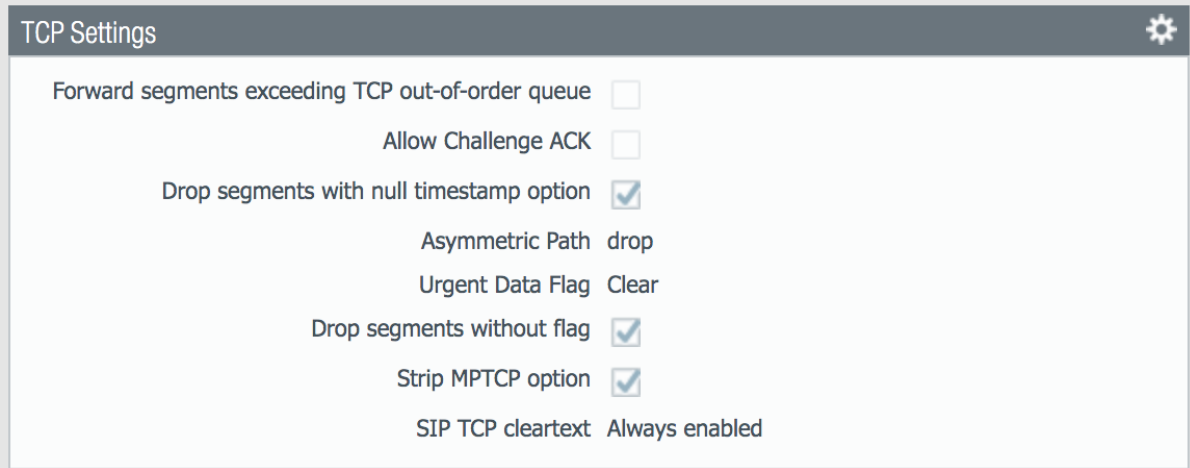
☐

Multicast Route Setup Buffer Size

1000

Key configuration elements:

- **Rematch Sessions:** cause the firewall to apply newly configured security policies to sessions that are already in progress

**Device > Setup > Session > TCP Settings**

TCP Settings	
Forward segments exceeding TCP out-of-order queue	<input type="checkbox"/>
Allow Challenge ACK	<input type="checkbox"/>
Drop segments with null timestamp option	<input checked="" type="checkbox"/>
Asymmetric Path	drop
Urgent Data Flag	Clear
Drop segments without flag	<input checked="" type="checkbox"/>
Strip MPTCP option	<input checked="" type="checkbox"/>
SIP TCP cleartext	Always enabled

Prevent TCP and MPTCP evasions

- set **Forward segments exceeding TCP out-of-order queue** to 'no'
- set **Drop segments with null timestamp option** to 'yes'
- set **urgent data flag** to 'clear'
- set **drop segments without flag** to 'yes'
- set **Strip MPTCP option** to 'yes'

## 5.1.2 Administrators

### IronSkillet default admin

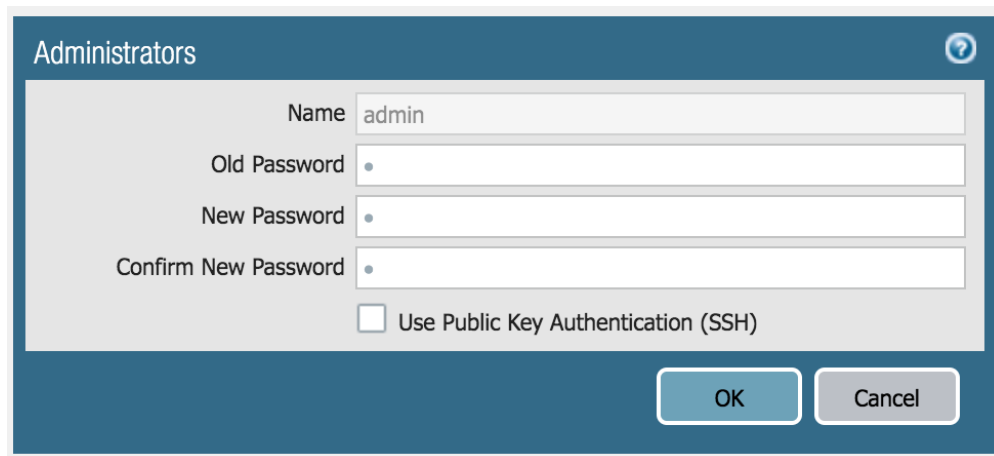
---

#### See also

General configuration information in the Admin Guide: [Device - Administrators](#)

---

Device > Administrators : admin

A screenshot of a web-based configuration dialog box titled "Administrators". The dialog has a dark blue header with a question mark icon in the top right. The main area is light gray and contains four input fields: "Name" with the text "admin", "Old Password", "New Password", and "Confirm New Password", each preceded by a label and a small blue dot icon. Below these fields is a checkbox labeled "Use Public Key Authentication (SSH)". At the bottom right, there are two buttons: "OK" and "Cancel".

The default reference configuration uses the default admin/admin login credentials. This should be changed immediately.

---

**Note:** As of release 9.0.4 the user is forced to change the admin password based on a minimum character length of 8 as part of a default password complexity profile. Once IronSkillet is loaded, this complexity profile is more complex overriding the default profile.

---

### 5.1.3 Response Pages

Response pages are the web pages that display when a user tries to access a URL.

---

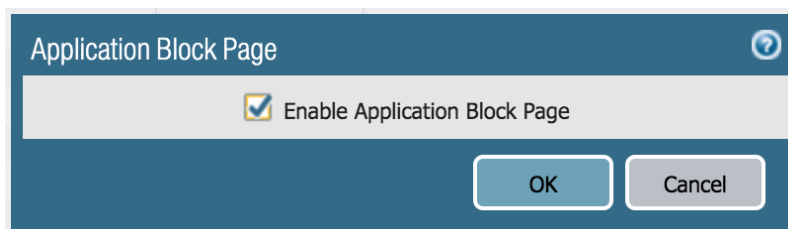
#### See also

General configuration information in the Admin Guide: [Device - Response Pages](#)

---

#### IronSkillet Enable Block Page

Device > Response Pages > Application Block Page

A screenshot of a web-based configuration dialog box titled "Application Block Page". The dialog has a dark blue header with a question mark icon in the top right. The main area is light gray and contains a single checkbox labeled "Enable Application Block Page" which is checked. At the bottom right, there are two buttons: "OK" and "Cancel".

Response pages display when a user attempts to access a URL that is not permitted by policy or content (threat) inspection. It is recommended to enable the **Application Block Page** setting so that users are aware of why an application is not working.

## 5.1.4 Log Settings

### See also

General configuration information in the Admin Guide: [Device - Log Settings](#)

There are multiple sections that can be configured for device log forwarding (System, Configuration, User-ID, and HIP Match)

Options include sending all logs, logs by severity, and custom attributes using the filter builder. Iron Skillet recommended settings include forwarding critical system logs to email and using Syslog for all system logs

Configuration, User-ID, and HIP Match should forward all logs to syslog

It is recommended to forward all logs to Panorama if the firewall is being managed by Panorama. This setting is unchecked as the Iron Skillet configuration assumes a standalone configuration

**Note:** Since log settings are operational and may vary across user environments, these are focused as 'reference configurations' as part of a recommended day one starter configuration.

### System

System event log actions

#### Device > Log Settings > System

System				
<input type="checkbox"/> Name	Description	Filter	Email	Syslog
<input type="checkbox"/> <a href="#">Email_Critical_System_Logs</a>	Email Critical System Logs	(severity eq critical)	Sample_Email_Profile	
<input type="checkbox"/> <a href="#">System_Log_Forwarding</a>		All Logs		Sample_Syslog_Profile

**Email\_Critical\_System\_Logs:** Send output as an email using a configured email profile. Only email severity=critical events

**System\_Log\_Forwarding:** As reference, forward all system logs as syslog using a configured syslog profile

Profiles configurations are in the section [Server Profiles](#).

### Configuration

Configuration event log actions

#### Device > Log Settings > Configuration

Configuration			
<input type="checkbox"/> Name	Description	Filter	Syslog
<input type="checkbox"/> <a href="#">Configuration_Log_Forwarding</a>		All Logs	Sample_Syslog_Profile

**Configuration\_Log\_Forwarding:** As reference, forward all configuration logs as syslog using a configured syslog profile

Profiles configurations are in the section *Server Profiles*.

## User-ID

User-ID event log actions

### Device > Log Settings > User-ID

User-ID			
<input type="checkbox"/>	Name	Description	Syslog
<input type="checkbox"/>	User-ID_Log_Forwarding		Sample_Syslog_Profile

**User-ID\_Log\_Forwarding:** As reference, forward all user ID logs as syslog using a configured syslog profile

Profiles configurations are in the section *Server Profiles*.

## Host Information Profile (HIP) Match

GlobalProtect HIP event log actions

### Device > Log Settings > HIP Match

HIP Match			
<input type="checkbox"/>	Name	Description	Syslog
<input type="checkbox"/>	HIP_Log_Forwarding		Sample_Syslog_Profile

## HIP\_Log\_Forwarding

As reference, forward all HIP logs as syslog using a configured syslog profile

Profiles configurations are in the section *Server Profiles*.

## 5.1.5 Server Profiles

---

### See also

General configuration information in the Admin Guide: [Device - Server Profiles](#)

---

---

**Note:** Since are operational and may vary across user environments, these are focused as ‘reference configurations’ as part of a recommended day one starter configuration.

---

**Note:** These values will need to be adjusted to the actual customer environment settings. You will want to verify that the Email Relay and Syslog machine can receive messages from the firewalls management interface (default **Service Route Configuration – Device > Setup > Services**).

Configuration of server profiles used by the log setting configurations.

## Syslog

### Device > Server Profiles > Syslog

Name	Syslog Server	Transport	Port	Format	Facility
Sample_Syslog	192.0.2.2	UDP	514	BSD	LOG_USER

Sample Syslog Profile using standard port 514.

**Note:** The sample IP address 192.0.2.2 is a non-routable address

## Email Server

## Device &gt; Server Profiles &gt; Email

Sample email server profile for critical alert events.

**Note:** the from/to and gateway values are reference only. The gateway address is non-routable.

## 5.1.6 Dynamic Updates

### See also

General configuration information in the Admin Guide: [Device - Dynamic Updates](#)

### IronSkillet Dynamic Updates

Dynamic updates allow the firewall to periodically check for content updates. Without this schedule configured, no new signature, vulnerabilities, malicious domains, or GlobalProtect files will be locally loaded into the firewall.

### Device > Dynamic Updates : schedules

Version ▲	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed
▶ Antivirus	Last checked: 2019/10/08 14:04:03 UTC		Schedule: Every hour at 4 minutes past the hour (Download and Install)				
▶ Applications and Threats	Last checked: 2019/10/08 14:32:03 UTC		Schedule: Every 30 minutes at 2 minutes past half-hour (Download and Install)				
▶ GlobalProtect Clientless VPN	Last checked: 2019/10/08 13:50:05 UTC		Schedule: Every hour at 50 minutes past the hour (Download and Install)				
▶ GlobalProtect Data File			Schedule: Every hour at 40 minutes past the hour (Download and Install)				
▶ WildFire	Last checked: 2019/10/08 14:46:04 UTC		Schedule: Every minute (Download and Install)				

Updates are configured with minimum time values to ensure new content loads are applied when available. They are also installed at the time of download.

Time schedules are varied around the hour to avoid download/install overlap between update types.

## Antivirus

Includes new and updated antivirus signatures, including signatures discovered by WildFire. You must have a Threat Prevention subscription to get these updates. New antivirus signatures are published daily.

## Applications and Threats

Includes new and updated application and threat signatures. This update is available if you have a Threat Prevention subscription (and in this case you will get this update instead of the Applications update). New Applications and Threats updates are published weekly. This means that the latest content update always includes the application and threat signatures released in previous versions.

## WildFire

Provides near real-time malware and antivirus signatures created as a result of the analysis done by the WildFire public cloud. WildFire signature updates are made available every five minutes. You can set the firewall to check for new updates as frequently as every minute to ensure that the firewall retrieves the latest WildFire signatures within a minute of availability. Without the WildFire subscription, you must wait 24 to 48 hours for the WildFire signatures to roll into the Applications and Threat update.

## GlobalProtect Clientless VPN

Contains new and updated application signatures to enable Clientless VPN access to common web applications from the GlobalProtect portal. You must have a GlobalProtect subscription to receive these updates. In addition, you must create a schedule for these updates before GlobalProtect Clientless VPN will function.

## GlobalProtect Data File

Contains the vendor-specific information for defining and evaluating host information profile (HIP) data returned by GlobalProtect apps. You must have a GlobalProtect gateway subscription in order to receive these updates. In addition, you must create a schedule for these updates before GlobalProtect will function.

# 5.2 Network

## 5.2.1 Network Profiles

---

### See also

General configuration information in the Admin Guide: [Network - Network Profiles](#)

---

## Zone Protection

IronSkillet includes ‘non volumetric’ recommendations that are device and deployment specific. This is configured as the Recommended\_Zone\_Protection profile and should be added to configured zones.

---

**Note:** IronSkillet does not include zone configurations so the user must apply this profile when configured zones.

---

**Network > Network Profiles > Zone Protection Profile > Recommended\_Zone\_Protection > Reconnaissance Protection**

The screenshot shows the 'Zone Protection Profile' configuration page. The 'Name' field is 'Recommended\_Zone\_Protection'. The 'Description' field is empty. The 'Reconnaissance Protection' tab is selected. Below the tabs is a table with the following data:

Scan	Enable	Action	Interval (sec)	Threshold (events)
TCP Port Scan	<input checked="" type="checkbox"/>	alert	2	100
Host Sweep	<input checked="" type="checkbox"/>	alert	10	100
UDP Port Scan	<input checked="" type="checkbox"/>	alert	2	100

TCP Port Scan, Host Sweep, and UDP Port Scan are enabled in alert-only mode to monitoring without blocking.

**Note:** Active blocking requires network tuning.

**Network > Network Profiles > Zone Protection Profile > Recommended\_Zone\_Protection > Packet Based Attack Protection > IP Drop**

The screenshot shows the 'Zone Protection Profile' configuration page. The 'Name' field is 'Recommended\_Zone\_Protection'. The 'Description' field is empty. The 'Packet Based Attack Protection' tab is selected. Below the tabs is the 'IP Drop' sub-tab. The 'IP Drop' sub-tab is selected. The following settings are visible:

- ☒ Spoofed IP address
- ☐ Strict IP Address Check
- ☐ Fragmented traffic
- IP Option Drop**
  - ☐ Strict Source Routing
  - ☐ Loose Source Routing
  - ☐ Timestamp
  - ☐ Record Route
  - ☐ Security
  - ☐ Stream ID
  - ☐ Unknown
  - ☒ Malformed

IP Drop settings enabled for a spoofed IP address and malformed packets.

**Network > Network Profiles > Zone Protection Profile > Recommended\_Zone\_Protection > Packet Based Attack Protection > TCP Drop**

The screenshot shows the 'Zone Protection Profile' configuration window. The 'Name' field is 'Recommended\_Zone\_Protection'. The 'Description' field is empty. The 'Packet Based Attack Protection' tab is selected. Under this tab, the 'TCP Drop' sub-tab is active. The settings for TCP Drop are as follows:

- ☐ Mismatched overlapping TCP segment
- ☐ Split Handshake
- ☒ TCP SYN with Data
- ☒ TCP SYNACK with Data
- Reject Non-SYN TCP:
- Asymmetric Path:
- Strip TCP Options**
  - ☒ TCP Timestamp
  - ☐ TCP Fast Open
  - Multipath TCP (MPTCP) Options:

TCP Drop settings enabled for TCP SYN with Data, SYNACK with Data. Also to strip TCP Timestamp.

**Note:** These are explicit enables in the template to ensure not disabled across software versions.

## 5.3 Objects

This section includes various profiles, objects, and tags used primarily in security and decryption policies.

### 5.3.1 Address

#### See also

General configuration information in the Admin Guide: [Objects - Addresses](#)

#### IronSkillet Address Objects

**Objects > Addresses : sinkholes**

	Name	Type	Address
<input type="checkbox"/>	Sinkhole-IPv4	FQDN	sinkhole.paloaltonetworks.com
<input type="checkbox"/>	Sinkhole-IPv6	IP Netmask	2600:5200::1

IronSkillet provides two address objects reference in security policies. These are associated to the sinkhole addresses used in the *Anti-Spyware* setting.

---

**Note:** 8.x releases use type of IP Netmask whereas 9.0 requires an FQDN entry for the sinkhole address.

---

### 5.3.2 Tags


---

**See also**

General configuration information in the Admin Guide: [Objects - Tags](#)

---

**IronSkillet Tag Objects****Object > Tags : directionals and version**

<input type="checkbox"/>	Name	Location	Color	Comments
<input type="checkbox"/>	Sanctioned	Predefined	 Olive	
<input type="checkbox"/>	empty	Predefined		
<input type="checkbox"/>	Outbound			Outbound to the Internet
<input type="checkbox"/>	Inbound			Inbound from the Internet
<input type="checkbox"/>	Internal			Internal to Internal
<input type="checkbox"/>	iron-skillet-version			version 0.0.3 for 9.0: version of this IronSkillet template file

Reference tags used in security policies along with an 'IronSkillet' version tag.

- **Outbound:** traffic from internal to external
- **Inbound:** traffic from external to internal
- **Internal:** internal-only traffic

---

**Note:** The iron-skillet-version tag is used for release tracking only.

---

### 5.3.3 Custom Objects

---

**See also**

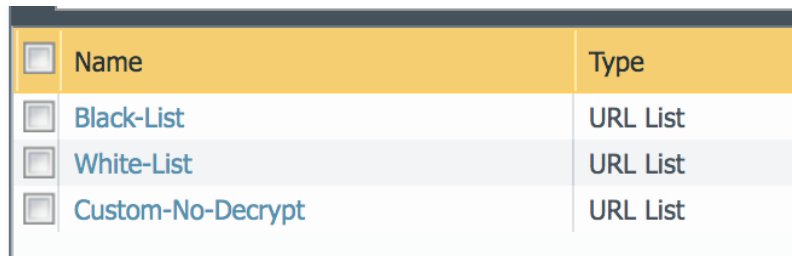
General configuration information in the Admin Guide: [Objects - Custom Objects](#)

---

User generated objects as placeholders.

## IronSkillet Custom Objects

### Object > Custom Objects > URL Category



<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Black-List	URL List
<input type="checkbox"/>	White-List	URL List
<input type="checkbox"/>	Custom-No-Decrypt	URL List

Placeholder for custom url categories used in security rules and url profiles. Using these categories prevents the need to modify the default template.

- **Black-List:** placeholder to be used in block rules and objects to override default template behavior
- **White-List:** placeholder to be used in permit rules and objects to override default template behavior
- **Custom-No-Decrypt:** to be used in the decryption no-decrypt rule to specify URLs that should no be decrypted

## 5.3.4 Security Profiles

### See also

General configuration information in the Admin Guide: [Objects - Security Profiles](#)

Security profiles in IronSkillet are explicitly named using one or more of the following:

- **Outbound:** traffic originating inside the network accessing external sites
- **Inbound:** traffic originating outside the network accessing internal sites
- **Internal:** traffic originating inside the network access other internal sites
- **Exception:** user-defined profile that can be used without changing the base profiles
- **Alert-Only:** alert-only for any traffic sessions; not recommended when blocking required

## AntiVirus

Antivirus profiles to protect against worms, viruses, and trojans and to block spyware downloads.

Outbound, Inbound, and Internal AntiVirus (AV) profiles.

## Object &gt; Security Profiles &gt; Antivirus : Blocking

<input type="checkbox"/>	Name	Packet Capture	Decoders		
			Name	Action	WildFire Action
<input type="checkbox"/>	Outbound-AV	<input type="checkbox"/>	http	reset-both	reset-both
			http2	reset-both	reset-both
			smtp	reset-both	reset-both
			imap	reset-both	reset-both
			pop3	reset-both	reset-both
			ftp	reset-both	reset-both
			smb	reset-both	reset-both
<input type="checkbox"/>	Inbound-AV	<input type="checkbox"/>	http	reset-both	reset-both
			http2	reset-both	reset-both
			smtp	reset-both	reset-both
			imap	reset-both	reset-both
			pop3	reset-both	reset-both
			ftp	reset-both	reset-both
			smb	reset-both	reset-both
<input type="checkbox"/>	Internal-AV	<input type="checkbox"/>	http	reset-both	reset-both
			http2	reset-both	reset-both
			smtp	reset-both	reset-both
			imap	reset-both	reset-both
			pop3	reset-both	reset-both
			ftp	reset-both	reset-both
			smb	reset-both	reset-both

These are all explicitly set to reset-both for all decoders.

## Object &gt; Security Profiles &gt; Antivirus : Alert-Only

<input type="checkbox"/>	Name	Packet Capture	Decoders		
			Name	Action	WildFire Action
<input type="checkbox"/>	Alert-Only-AV	<input type="checkbox"/>	http	alert	alert
			http2	alert	alert
			smtp	alert	alert
			imap	alert	alert
			pop3	alert	alert
			ftp	alert	alert
			smb	alert	alert

Sets all decoders to alert mode.

**Object > Security Profiles > Antivirus : Exception**

<input type="checkbox"/> Name ▲	Packet Capture	Decoders		
		Name	Action	WildFire Action
<input type="checkbox"/> Exception-AV	<input type="checkbox"/>	http	reset-both	default (reset-both)
		http2	reset-both	default (reset-both)
		smtp	reset-both	reset-both
		imap	reset-both	reset-both
		pop3	reset-both	reset-both
		ftp	reset-both	default (reset-both)
		smb	reset-both	default (reset-both)

Set in blocking mode as default. This profile is a placeholder to be customized by the user and used in security profile groups and policies without the need to edit the IronSkillet blocking profiles.

**Anti-Spyware**

Anti-Spyware profiles to block attempts from spyware on compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.

**Object > Security Profiles > Antivirus : Outbound-AS****Rules: Outbound Anti-Spyware (AS) and Inbound-AS profiles**

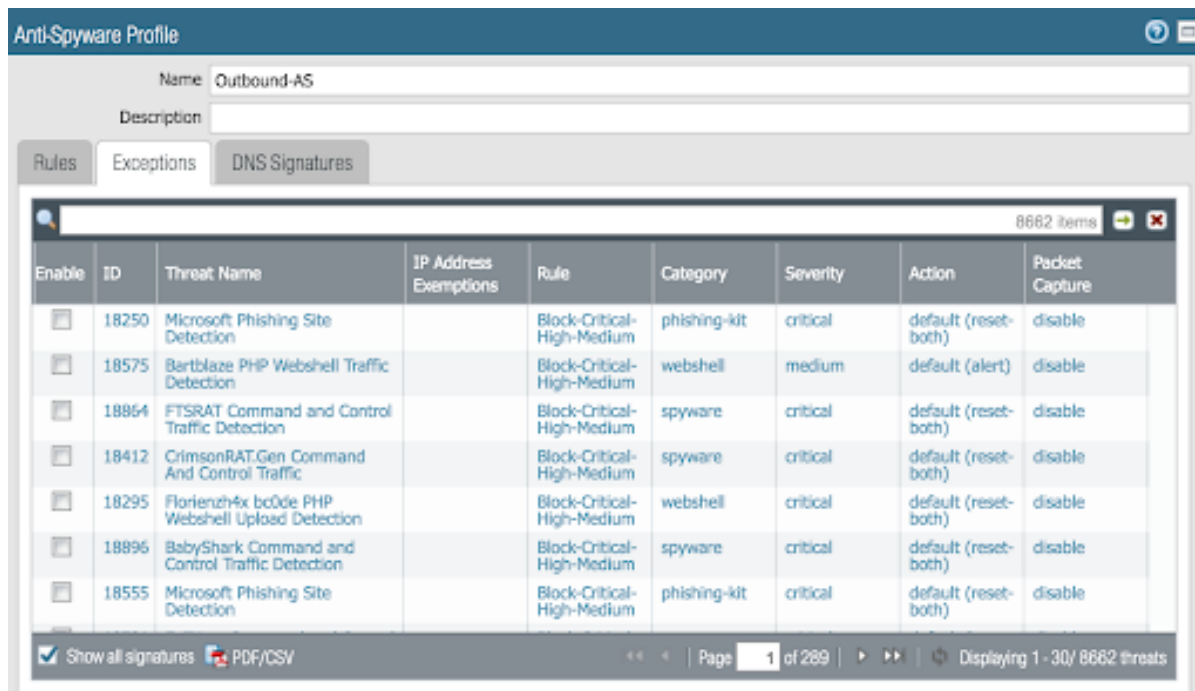
Anti-Spyware Profile				
Name		Outbound-AS		
Description				
Rules		Exceptions DNS Signatures		
<input type="checkbox"/> Rule Name	Severity	Action	Packet Capture	
<input type="checkbox"/> Block-Critical-High-Medium	high	reset-both	single-packet	
	critical			
	medium			
<input type="checkbox"/> Default-Low-Info	low	default	disable	
	informational			

Rules block critical, high, and medium severity events. For low and informational, default is used.

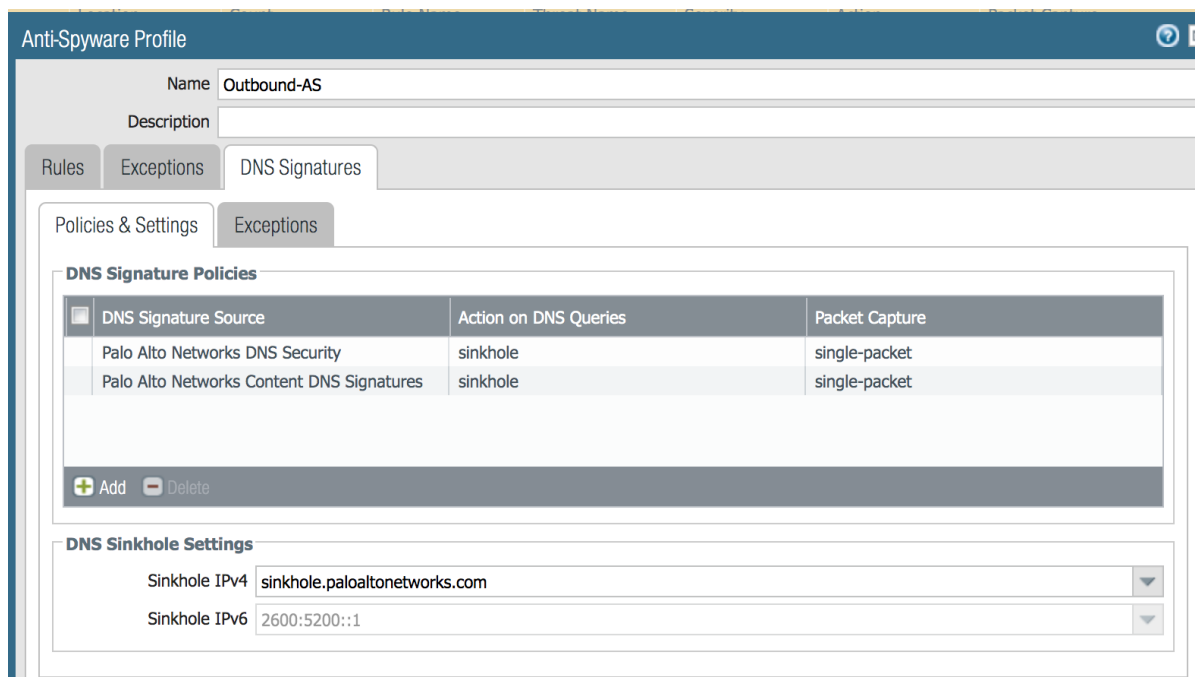
**Note:** Only Outbound-AS is shown with Inbound-AS having an identical configuration.

**Exceptions: Checking Default Actions**

To see the actions for 'default', click into Exceptions and enable 'Show all signatures'. The Action column shows default actions for each ID.



### DNS Signature: Sinkhole Malicious Domain Traffic



The profile also sinkholes malicious domains based on the sinkhole settings. The settings map to the address objects and sinkhole redirects can be dropped as part of the security policies if no sinkhole server is used.

**Note:** As of 9.0, instead of only leveraging a list of locally stored malicious domains (Content DNS Signatures), Palo Alto Networks also provides a DNS Security service subscription for cloud-based domain lookups.

**Object > Security Profiles > Antivirus : Internal-AS**

The Internal profile shifts the medium severity to ‘default’ instead of reset both slightly lowering the security posture for internal-only sessions.

The screenshot shows the 'Anti-Spyware Profile' configuration window for 'Internal-AS'. The 'Rules' tab is selected, displaying a table of rules. The 'Rules' tab is active, and the 'Exceptions' and 'DNS Signatures' tabs are also visible.

Rule Name	Severity	Action	Packet Capture
Block-Critical-High	high critical	reset-both	single-packet
Default-Medium-Low-Info	low informational medium	default	disable

The DNS Signatures configuration is the same as Outbound-AS and Inbound-AS.

The screenshot shows the 'Anti-Spyware Profile' configuration window for 'Internal-AS'. The 'DNS Signatures' tab is selected, displaying the 'DNS Signature Policies' and 'DNS Sinkhole Settings' sections.

**DNS Signature Policies**

DNS Signature Source	Action on DNS Queries	Packet Capture
Palo Alto Networks DNS Security	sinkhole	single-packet
Palo Alto Networks Content DNS Signatures	sinkhole	single-packet

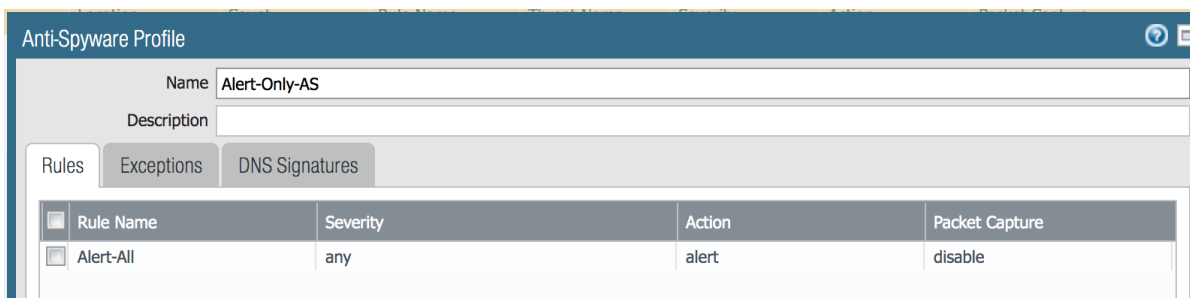
**DNS Sinkhole Settings**

Sinkhole IPv4: sinkhole.paloaltonetworks.com

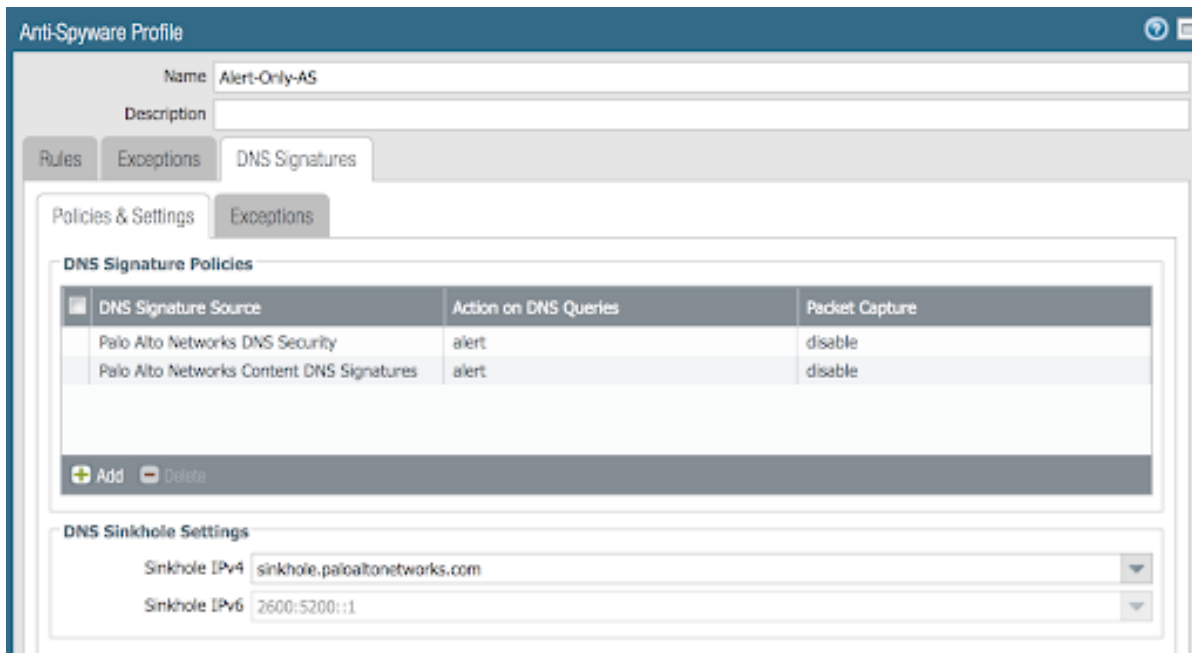
Sinkhole IPv6: 2600:5200::1

**Object > Security Profiles > Antivirus : Alert-Only**

This is a non-blocking alert-only configuration that can be used for testing/demonstration purposes.

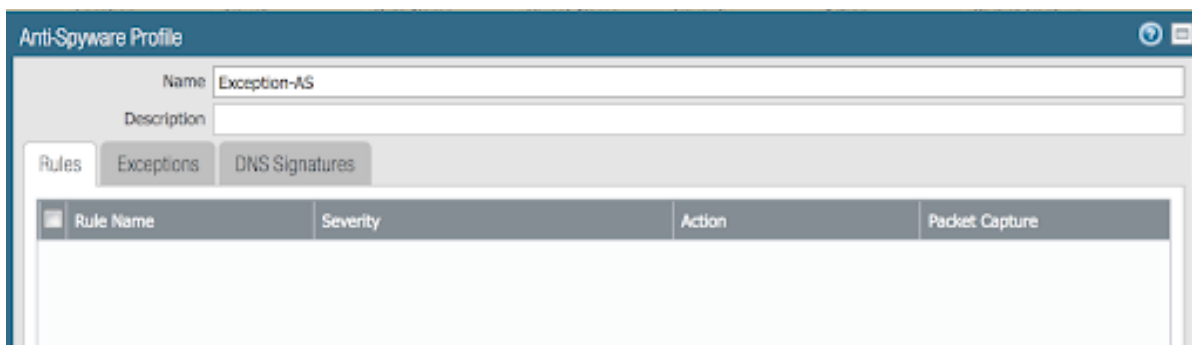


The malicious domain actions are also 'alert' for monitoring purposes only.



## Object > Security Profiles > Antivirus : Exception-AS

This is a placeholder allowing for custom rules without editing the base template configuration profiles. The exception placeholder contains no preconfigured rules.



## Vulnerability

Vulnerability protection profiles to stop attempts to exploit system flaws or gain unauthorized access to systems.

**Object > Security Profiles > Vulnerability Protection : Outbound-VP**

**Vulnerability Protection Profile**

Name: Outbound-VP

Description:

Rules

Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
<input type="checkbox"/> Block-Critical-High-Medium	any	any	any	critical high medium	reset-both	single-packet
<input type="checkbox"/> Default-Low-Info	any	any	any	low informational	default	disable

IronSkillet adds two rules:

- (1) reset-both for critical/high/medium severity events
- (2) the use of default actions for low and informational severities.

**Object > Security Profiles > Vulnerability Protection : Inbound-VP**

**Vulnerability Protection Profile**

Name: Inbound-VP

Description:

Rules

Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
<input type="checkbox"/> Block-Critical-High-Medium	any	any	any	critical high medium	reset-both	single-packet
<input type="checkbox"/> Default-Low-Info	any	any	any	low informational	default	disable

Currently identical to the above Outbound profile to block critical/high/medium and use 'default' for low and informational severities.

**Object > Security Profiles > Vulnerability Protection : Internal-VP**

Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
Block-Critical-High	any	any	any	critical	reset-both	single-packet
Default-Medium-Low-Info	any	any	any	low informational medium	default	disable

As with the Anti-spyware internal profile, medium is set as ‘default’ along with low and informational. This adds some trust to internal-only communications.

**Object > Security Profiles > Vulnerability Protection : Alert-Only-VP**

Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
Alert-All	any	any	any	any	alert	disable

Alert-Only provides a monitoring-only profile for vulnerability events. It is designed for use in demonstration or test deployments without active blocking.

**Object > Security Profiles > Vulnerability Protection : Exception-VP**

Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
-----------	-------------	-----	-----------	----------	--------	----------------

This profile is a placeholder only allowing a user to customize their own ruleset without modifying the default Iron-Skillet profiles.

## URL Filtering

URL filtering profiles to restrict users access to specific websites and/or website categories, such as shopping or gambling.

### Object > Security Profiles > URL-Filtering

<input type="checkbox"/> Name	Location	Site Access	User Credential Submission
<input type="checkbox"/> default	Predefined	Allow Categories (58) Alert Categories (3) Continue Categories (0) Block Categories (9) Override Categories (0)	Allow Categories (70) Alert Categories (0) Continue Categories (0) Block Categories (0)
<input type="checkbox"/> Outbound-URL		Allow Categories (0) Alert Categories (67) Continue Categories (0) Block Categories (5) Override Categories (0)	Allow Categories (0) Alert Categories (0) Continue Categories (0) Block Categories (72)
<input type="checkbox"/> Alert-Only-URL		Allow Categories (0) Alert Categories (72) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (0) Alert Categories (72) Continue Categories (0) Block Categories (0)
<input type="checkbox"/> Exception-URL		Allow Categories (0) Alert Categories (67) Continue Categories (0) Block Categories (5) Override Categories (0)	Allow Categories (0) Alert Categories (0) Continue Categories (0) Block Categories (72)

IronSkillet provides only 3 profiles for URL excluding the Inbound and Internal used in the other profiles. The IronSkillet assumption is that only outbound requests may be accessing malicious sites.

### Object > Security Profiles > URL-Filtering : Outbound-URL

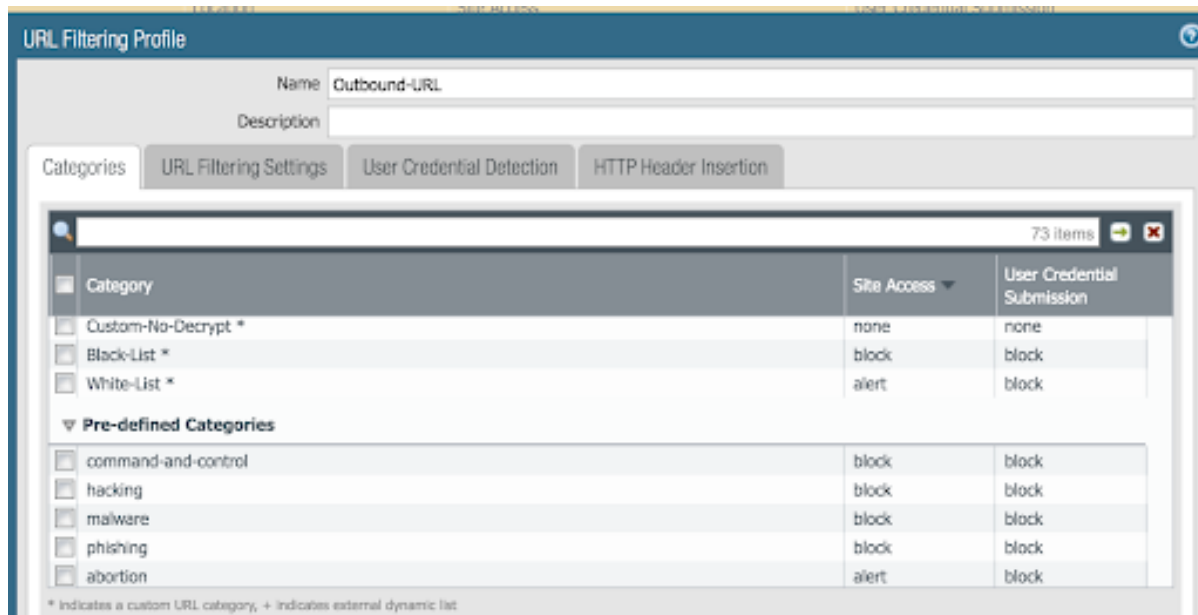
#### Categories: Site Access

IronSkillet only blocks known malicious categories and not high risk categories such as copyright-infringement mentioned in our Best Practice Assessment (BPA).

Categories blocked in the Outbound and Exception profiles:

- Malware
- Command-and-Control
- Phishing
- Hacking
- Black-List [custom object users can edit]

All other categories have their action set as 'alert' instead of the default 'allow' for logging purposes.



### Categories: User Credential Submission

If you block all the URL categories in a URL Filtering profile for user credential submission, you don't need to check credentials. IronSkillet takes this approach blocking all categories under User Credential Submission.

The Alert-Only-URL profile sets all actions to alert for logging purposes, include User Credential Submission. No categories are blocked.

### File Blocking

This set of profiles allow the NGFW to explicitly block files transiting the firewall by type and direction.

### Object > Security Profiles > File-Blocking

Name	Rule Name	Applications	File Types	Direction	Action
<input type="checkbox"/> basic file blocking	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, oox, pdf, ppt, rar, sct, torrent, vbe, wsf	both	block
	Continue prompt encrypted files	any	encrypted-ox, encrypted-zip	both	continue
	Log all other file types	any	both	both	alert
<input type="checkbox"/> strict file blocking	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, oox, pdf, ppt, rar, sct, tar, torrent, vbe, wsf	both	block
	Block encrypted files	any	encrypted-ox, encrypted-zip	both	block
	Log all other file types	any	both	both	alert
<input type="checkbox"/> Outbound-FB	Alert-All	any	any	both	alert
	Block	any	7z, bat, chm, class, cpl, dll, hlp, hta, jar, oox, pdf, sct, torrent, vbe, wsf	both	block
<input type="checkbox"/> Inbound-FB	Alert-All	any	any	both	alert
	Block	any	7z, bat, chm, class, cpl, dll, hlp, hta, jar, oox, pdf, sct, torrent, vbe, wsf	both	block
<input type="checkbox"/> Internal-FB	Alert-All	any	any	both	alert
	Block	any	7z, bat, chm, class, cpl, dll, hlp, hta, jar, oox, pdf, sct, torrent, vbe, wsf	both	block
<input type="checkbox"/> Alert-Only-FB	Alert-Only	any	any	both	alert

IronSkillet defines a day one perspective without variations in file blocking based on URL category, direction, or application. File types that are not blocked are set as 'alert' for logging purposes.

The set of blocked file types represents the most common malicious file types that typically are not expected to cross a security zone boundary. Other types are ignored (eg. exe) since these can be used for legitimate, although not recommended, business purposes.

**Note:** Supported WildFire file types, even if blocked, will be sent to WildFire for analysis if Wildfire is license and configured in the device.

## WildFire Analysis

WildFire™ analysis profiles to specify for file analysis to be performed locally on the WildFire appliance or in the WildFire cloud. IronSkillet uses the cloud option.

### Object > Security Profiles > WildFire Analysis

<input type="checkbox"/>	Name	Rule Name	Applications	File Types	Direction	Analysis
<input type="checkbox"/>	default	default	any	any	both	public-cloud
<input type="checkbox"/>	Outbound-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Inbound-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Internal-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Alert-Only-WF	Forward-All	any	any	both	public-cloud

All profiles are set to send all file types for all applications in any direction to WildFire for analysis.

This configuration is for file analysis only. WildFire signatures and protections are configured in the Anti-Virus profile. Below is the reference example for the Outbound-AV profile.

Antivirus Profile

Name

Outbound-AV

Description

Antivirus

Virus Exception

☐ Packet Capture

Decoders

Decoder	Action	WildFire Action
ftp	reset-both	reset-both
http	reset-both	reset-both
http2	reset-both	reset-both
imap	reset-both	reset-both
pop3	reset-both	reset-both
smb	reset-both	reset-both
smtp	reset-both	reset-both

Based on the dynamic updates configuration, the device will check for new WildFire content updates based on world-wide analysis every minute to download the latest five minute release. These signatures are moved to the antivirus signature set on a daily basis for customers not subscribing to the WildFire service.

## 5.3.5 Security Profile Groups

---

### See also

General configuration information in the Admin Guide: [Objects - Security Profile Groups](#)

---

In addition to individual profiles, you can combine profiles that are often applied together, and create Security Profile Groups. These can be referenced in a security profile without the need to explicitly reference each profile.

### IronSkillet Security Profile Groups

#### Object > Security Profile Groups : all groups

<input type="checkbox"/>	Name	Antivirus Profile	Anti-Spyware Profile	Vulnerability Protection Profile	URL Filtering Profile	File Blocking Profile	WildFire Analysis Profile
<input type="checkbox"/>	Outbound	Outbound-AV	Outbound-AS	Outbound-VP	Outbound-URL	Outbound-FB	Outbound-WF
<input type="checkbox"/>	Inbound	Inbound-AV	Inbound-AS	Inbound-VP		Inbound-FB	Inbound-WF
<input type="checkbox"/>	Internal	Internal-AV	Internal-AS	Internal-VP		Internal-FB	Internal-WF
<input type="checkbox"/>	Alert-Only	Alert-Only-AV	Alert-Only-AS	Alert-Only-VP	Alert-Only-URL	Alert-Only-FB	Alert-Only-WF
<input type="checkbox"/>	default	Outbound-AV	Outbound-AS	Outbound-VP	Outbound-URL	Outbound-FB	Outbound-WF

Each profile group is associated to the set of profiles reference the same direction or ‘alert’ mode.

The default profile, based on the Outbound security profiles, is created so that new security policies can easily reference this default profile group.

IronSkillet does not reference the security profile objects since IronSkillet does not have explicit allow rules.

## 5.3.6 Log Forwarding

---

### See also

General configuration information in the Admin Guide: [Objects - Log Forwarding](#)

---

Sets up log forwarding profiles referenced in security policies.

### IronSkillet Log Forwarding

**Object > Log Forwarding : default**

Log Forwarding Profile

Name

default

Description

<input type="checkbox"/>	Name	Log Type	Filter	Forward Method
<input type="checkbox"/>	Traffic_Log_Forwarding	traffic	All Logs	<b>SysLog</b> <ul style="list-style-type: none"> <li>Sample_Syslog_Profile</li> </ul>
<input type="checkbox"/>	Threat_Log_Forwarding	threat	All Logs	<b>SysLog</b> <ul style="list-style-type: none"> <li>Sample_Syslog_Profile</li> </ul>
<input type="checkbox"/>	Email_Malicious_Verdicts	wildfire	(verdict eq malicious)	<b>Email</b> <ul style="list-style-type: none"> <li>Sample_Email_Profile</li> </ul>
<input type="checkbox"/>	Email_Phishing_Verdicts	wildfire	(verdict eq phishing)	<b>Email</b> <ul style="list-style-type: none"> <li>Sample_Email_Profile</li> </ul>
<input type="checkbox"/>	Wildfire_Log_Forwarding	wildfire	All Logs	<b>SysLog</b> <ul style="list-style-type: none"> <li>Sample_Syslog_Profile</li> </ul>
<input type="checkbox"/>	URL_Log_Forwarding	url	All Logs	<b>SysLog</b> <ul style="list-style-type: none"> <li>Sample_Syslog_Profile</li> </ul>
<input type="checkbox"/>	Data_Log_Forwarding	data	All Logs	<b>SysLog</b> <ul style="list-style-type: none"> <li>Sample_Syslog_Profile</li> </ul>
<input type="checkbox"/>	Tunnel_Log_Forwarding	tunnel	All Logs	<b>SysLog</b> <ul style="list-style-type: none"> <li>Sample_Syslog_Profile</li> </ul>
<input type="checkbox"/>	Auth_Log_Forwarding	auth	All Logs	<b>SysLog</b> <ul style="list-style-type: none"> <li>Sample_Syslog_Profile</li> </ul>

IronSkillet sets all log events to be sent to Syslog. Any malicious or phishing WildFire verdicts are emailed using the Threat Alert email profile. The Panorama associated configuration sends log to Panorama. Users can modify the default logging profile to send logs to additional locations as required.

The 'default' naming is used so that new security rules will automatically pick up this logging profile.

## 5.3.7 Decryption

Decryption profiles enable you to block and control specific aspects of SSL and SSH traffic that you have specified for decryption, as well as traffic that you have explicitly excluded from decryption. After you create a decryption profile, you can then add that profile to a decryption policy; any traffic matched to the decryption policy is additionally enforced based on the profile settings.

### Decryption Profile

#### See also

General configuration information in the Admin Guide: [Objects - Decryption Profile](#)

**Object > Decryption > Decryption Profile : Recommended\_Decryption\_Profile**

The Recommended\_Decryption\_Profile is provided to set several baseline, recommended profile elements.

**Decryption Profile > SSL Decryption : SSL Forward Proxy**

The screenshot shows the 'Decryption Profile' configuration window for the 'Recommended\_Decryption\_Profile'. The 'SSL Decryption' tab is selected, and within it, the 'SSL Forward Proxy' sub-tab is active. The 'Server Certificate Verification' section has five checked options: 'Block sessions with expired certificates', 'Block sessions with untrusted issuers', 'Block sessions with unknown certificate status', 'Block sessions on certificate status check timeout', and 'Restrict certificate extensions' (with a 'Details' link). The 'Append certificate's CN value to SAN extension' option is unchecked. The 'Unsupported Mode Checks' section has three checked options: 'Block sessions with unsupported versions', 'Block sessions with unsupported cipher suites', and 'Block sessions with client authentication'. The 'Failure Checks' section has two unchecked options: 'Block sessions if resources not available' and 'Block sessions if HSM not available'. The 'Client Extension' section has one unchecked option: 'Strip ALPN'.

If using SSL Forward Proxy, block sessions with invalid certs and versions.

## Decryption Profile &gt; SSL Decryption : SSL Protocol Settings

The screenshot shows the 'Decryption Profile' configuration window. The 'Name' field is 'Recommended\_Decryption\_Profile'. The 'SSL Decryption' tab is selected, and within it, the 'SSL Protocol Settings' sub-tab is active. The 'Protocol Versions' section has 'Min Version' set to 'TLSv1.2' and 'Max Version' set to 'Max'. The 'Key Exchange Algorithms' section has 'RSA' unchecked, 'DHE' checked, and 'ECDHE' checked. The 'Encryption Algorithms' section has '3DES' and 'RC4' unchecked, and 'AES128-CBC', 'AES256-CBC', 'AES128-GCM', and 'AES256-GCM' all checked. The 'Authentication Algorithms' section has 'MD5' and 'SHA1' unchecked, and 'SHA256' and 'SHA384' checked.

**Protocol versions:** Set the minimum protocol version to TLSv1.2. Any TLSv1.1 errors can help find outdated TLS endpoints

**Encryption Algorithms:** 3DES and RC4 not recommended and unavailable when TLSv1.2 is the minimum version.

**Authentication Algorithms:** MD5 not recommended and unavailable when TLSv1.2 is the minimum version

## Decryption Profile &gt; No Decryption

The screenshot shows the 'Decryption Profile' configuration window. The 'Name' field is 'Recommended\_Decryption\_Profile'. The 'No Decryption' tab is selected. The 'Server Certificate Verification' section has 'Block sessions with expired certificates' and 'Block sessions with untrusted issuers' both checked. A note at the bottom states: 'Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.'

Even without decrypting, the recommended profile can block session with invalid certs or untrusted issuers.

## 5.4 Policies

### 5.4.1 Security















See also

General configuration information in the Admin Guide: [Policies - Security](#)

## IronSkillet Security Policies

IronSkillet only provides suggested block rules and no traffic passing allow rules. When admins add new security rules, they should reference the security profile groups and logging profile configured under Objects.

### Policies > Security : edl and sinkhole

	Name	Tags	Source		Destination		Application	Service	URL Category	Action	Profile
			Zone	Address	Zone	Address					
1	Outbound Block Rule	Outbound	any	any	any	 Palo Alto Netw...  Palo Alto Netw...  Palo Alto Netw...	any	any	any	 Deny	none
2	Inbound Block Rule	Inbound	any	 Palo Alto Netw...  Palo Alto Netw...  Palo Alto Netw...	any	any	any	any	any	 Deny	none
3	DNS Sinkhole Block	Outbound	any	any	any	 Sinkhole-IPv4  Sinkhole-IPv6	any	any	any	 Deny	none
4	intrazone-default	none	any	any	(intrazone)	any	any	any	any	 Allow	
5	interzone-default	none	any	any	any	any	any	any	any	 Drop	none

**Inbound and Outbound Block Rules** Recommended Deny rules using the Palo Alto Networks predefined external dynamic lists (EDLs).

From Objects > External Dynamic Lists:

<input type="checkbox"/> Name	Location	Description	Source
▼ Dynamic IP Lists			
<input type="checkbox"/> <a href="#">Palo Alto Networks - Bulletproof IP addresses</a>	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.	Palo Alto Networks - Bulletproof IP addresses
<input type="checkbox"/> <a href="#">Palo Alto Networks - High risk IP addresses</a>	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	Palo Alto Networks - High risk IP addresses
<input type="checkbox"/> <a href="#">Palo Alto Networks - Known malicious IP addresses</a>	Predefined	IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.	Palo Alto Networks - Known malicious IP addresses

These external dynamic lists (EDLs) require a threat subscription and content update. Before configuring these security rules, the user needs to ensure that the EDLs show up under Objects - External Dynamic Lists. If not present, either the subscription is not valid or the content update has not been performed.

**DNS Sinkhole Block** This policy rule lets the firewall drop sinkhole redirected traffic as defined in the Spyware object profiles. DNS lookups matching a malicious domain will be sinkholed.

If the admin chooses to allow the traffic to pass to a legitimate sinkhole, this rule can be disabled or removed.

## 5.4.2 Decryption

---

**See also**

General configuration information in the Admin Guide: [Policies - Decryption](#)

---

## IronSkillet Decryption Policies

The IronSkillet decryption policies contain two rules: (1) An optional no-decrypt URL category rule to bypass recommended URL categories when SSL decrypt is enabled and (2) a default NO-Decrypt rule that only provides certificate validation checks according to the Recommended\_Decryption\_Profile.

Neither of the two rules perform any decryption but rather validate the encrypted sessions (SSL/SSH) meet particular integrity and encryption standards.

### Policies > Decryption : no decrypt

	Name	Tags	Source	Destination	URL Category	Service	Decrypt Options		
			Zone	Zone			Action	Type	Decryption Profile
1	NO-Decrypt URL Cat...	none	any	any	financial-services government health-and-med... Custom-No-Decr...	any	no-decrypt	ssl-forward-proxy	Recommended_Decryp...
2	NO-Decrypt Rule	none	any	any	any	any	no-decrypt	ssl-forward-proxy	Recommended_Decryp...

SSL Decryption is highly recommended to gain visibility to traffic sessions yet is not part of the IronSkillet configuration template due to various requirements around certificates and application testing before full implementations. Therefore as a Day One broad usage template, SSL decrypt is bypassed with only reference rules and profiles.

## 5.5 Monitor

### 5.5.1 Manage Custom Reports

---

**See also**

General configuration information in the Admin Guide: [Monitor - Custom Reports](#)

---

## IronSkillet Custom Reports

IronSkillet includes a small set of custom reports aimed at SecOps practices and discovering malicious behavior. These can be used as a reference for additional custom reports.

## Monitor &gt; Manage Custom Reports

<input type="checkbox"/>	Name	Description	Database	Time Frame	R...	Sort By	Group By	Sche...
<input type="checkbox"/>	Host-visit malicious sites plus		URL Log	Last 7 Calendar Days	500	Count	src	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Hosts visit malicious sites		URL Log	Last 7 Calendar Days	500	Count	src	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Hosts visit questionable sites		URL Log	Last 7 Calendar Days	500	Count	src	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Host-visit quest sites plus	Detail of hosts visiting questionable URLs	URL Log	Last 7 Calendar Days	500	Count	src	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Wildfire malicious verdicts	Files uploaded or downloaded that were later found to be malicious. This is a summary. Act on real-time email.	WildFire Submissions	Last 30 Calendar Days	500	Count		<input checked="" type="checkbox"/>
<input type="checkbox"/>	Wildfire verdicts SMTP	Links sent from emails found to be malicious.	WildFire Submissions	Last 30 Calendar Days	500	Count		<input checked="" type="checkbox"/>
<input type="checkbox"/>	Clients sinkholed		Traffic Log	Last 30 Calendar Days	500	Count	from	<input checked="" type="checkbox"/>

## Monitor &gt; Management &gt; Custom Reports &gt; Host-visit malicious sites plus

Custom Report

Report Setting

Load Template

Run Now

Name

Host-visit malicious sites plus

Description

Database

URL Log

☒ Scheduled

Time Frame

Last 7 Calendar Days

Sort By

Count

Top 500

Group By

Source address

50 Groups

Available Columns

App Category

App Container

App Sub Category

App Technology

Application

Selected Columns

Source Zone

Source User

Category

Action

Count

Top

Up

Down

Bottom

Query Builder

(category eq command-and-control) or (category eq hacking) or (category eq malware) or (category eq phishing)

Filter Builder

OK

Cancel

A weekly report to identify over the past seven days the following categories:

- Command-and-control
- Hacking
- Malware
- Phishing

**Monitor > Management > Custom Reports > Host-visit malicious sites**

The screenshot shows the 'Custom Report' configuration window. The 'Report Setting' tab is active. The 'Name' field is 'Hosts visit malicious sites'. The 'Database' is 'URL Log'. The 'Time Frame' is 'Last 7 Calendar Days'. The 'Sort By' is 'Count' and 'Top 500'. The 'Group By' is 'Source address' and '50 Groups'. The 'Available Columns' list includes Action, App Category, App Container, App Sub Category, and App Technology. The 'Selected Columns' list includes Source Zone, Source User, and Count. The 'Query Builder' section contains the query: `(category eq command-and-control) or (category eq hacking) or (category eq malware) or (category eq phishing)`. The 'Filter Builder' button is visible. The 'OK' and 'Cancel' buttons are at the bottom right.

Custom Report

Report Setting

Load Template Run Now

Name: Hosts visit malicious sites

Description:

Database: URL Log

☒ Scheduled

Time Frame: Last 7 Calendar Days

Sort By: Count Top 500

Group By: Source address 50 Groups

Available Columns

- Action
- App Category
- App Container
- App Sub Category
- App Technology

Selected Columns

- Source Zone
- Source User
- Count

Top Up Down Bottom

Query Builder

(category eq command-and-control) or (category eq hacking) or (category eq malware) or (category eq phishing)

Filter Builder

OK Cancel

Same categories as previous report with fewer columns to simplify output

**Monitor > Management > Custom Reports > Hosts visit questionable sites**

**Custom Report**

Report Setting

Load Template Run Now

Name: Hosts visit questionable sites

Description:

Database: URL Log

☒ Scheduled

Time Frame: Last 7 Calendar Days

Sort By: Count Top 500

Group By: Source address 50 Groups

**Available Columns**

- Action
- App Category
- App Container
- App Sub Category
- App Technology

**Selected Columns**

- Source Zone
- Source User
- Count

**Query Builder**

(category eq dynamic-dns) and (category eq parked) and (category eq questionable) and (category eq unknown)

Filter Builder

OK Cancel

A weekly report to identify over the past seven days the following categories

- Dynamic-dns
- Parked
- Questionable
- Unknown

**Monitor > Management > Custom Reports > Host-visit quest sites plus**

The screenshot shows the 'Custom Report' configuration window. The 'Report Setting' tab is active. The report is named 'Host-visit quest sites plus' and is described as 'Detail of hosts visiting questionable URLs'. It uses the 'URL Log' database and is scheduled. The time frame is 'Last 7 Calendar Days'. It is sorted by 'Count' (Top 500) and grouped by 'Source address' (50 Groups). The 'Available Columns' list includes App Category, App Container, App Sub Category, App Technology, and Application. The 'Selected Columns' list includes Source Zone, Source User, Category, Action, and Count. The 'Query Builder' section contains the query: (category eq dynamic-dns) and (category eq parked) and (category eq questionable) and (category eq unknown). The 'Filter Builder' button is visible. The window has 'OK' and 'Cancel' buttons at the bottom right.

Report Setting		Available Columns	Selected Columns
Name	Host-visit quest sites plus	App Category	Source Zone
Description	Detail of hosts visiting questionable URLs	App Container	Source User
Database	URL Log	App Sub Category	Category
<input checked="" type="checkbox"/> Scheduled		App Technology	Action
Time Frame	Last 7 Calendar Days	Application	Count
Sort By	Count		
	Top 500		
Group By	Source address		
	50 Groups		

**Query Builder**

(category eq dynamic-dns) and (category eq parked) and (category eq questionable) and (category eq unknown)

[Filter Builder](#)

OK Cancel

**Note:** 'questionable' was concatenated to meet name length requirements

Same categories as previous report with more columns as an extended view

**Monitor > Management > Custom Reports > Wildfire malicious verdicts**

**Custom Report**

Report Setting

Load Template Run Now

Name: Wildfire malicious verdicts

Description: Files uploaded or downloaded that were later found to t

Database: WildFire Submissions

☒ Scheduled

Time Frame: Last 30 Calendar Days

Sort By: Count Top 500

Group By: None 10 Groups

**Available Columns**

- App Category
- App Sub Category
- App Technology
- Client to Server
- Day

**Selected Columns**

- File Digest
- + App Container
- Application
- Verdict
- File Type

Top Up Down Bottom

**Query Builder**

(app neq smtp) and (category neq benign)

Filter Builder

OK Cancel

Report viewing all grayware and malicious verdicts

- Minus smtp (SMTP in separate report)
- Minus benign (only grayware and malicious)

**Monitor > Management > Custom Reports > Wildfire verdicts SMTP**

Custom Report

Report Setting

Load Template Run Now

Name: Wildfire verdicts SMTP

Description: Links sent from emails found to be malicious.

Database: WildFire Submissions

☒ Scheduled

Time Frame: Last 30 Calendar Days

Sort By: Count Top 500

Group By: None 10 Groups

Available Columns	Selected Columns
App Category	File Digest
App Sub Category	<input checked="" type="checkbox"/> App Container
App Technology	<input checked="" type="checkbox"/> Application
Client to Server	Verdict
Count	File Type

Top Up Down Bottom

Query Builder

(app eq smtp) and (category neq benign)

Filter Builder

OK Cancel

Report viewing all grayware and malicious verdicts

- Only SMTP traffic
- Minus benign (only grayware and malicious)

**Monitor > Management > Custom Reports > Clients sinkholed**

The screenshot shows the 'Custom Report' configuration window. The 'Report Setting' tab is active. The 'Name' field is 'Clients sinkholed'. The 'Database' is 'Traffic Log'. The 'Scheduled' checkbox is checked. The 'Time Frame' is 'Last 30 Calendar Days'. The 'Sort By' is 'Count' and 'Top 500'. The 'Group By' is 'Source Zone' and '50 Groups'. The 'Available Columns' list includes Action, Action\_source, App Category, App Container, and App Sub Category. The 'Selected Columns' list includes Source address, Source User, and Count. The 'Query Builder' section contains the rule '(rule eq 'DNS Sinkhole Block')'. The 'Filter Builder' button is visible. The 'OK' and 'Cancel' buttons are at the bottom right.

The importance here is we are viewing the verdict based on a rule. Reason being that if you go to threat log and say (action eq sinkhole) it will give you the DNS server and not the culprit. This rule allows for identification of the compromised client.

## 5.5.2 PDF Reports

### See also

General configuration information in the Admin Guide: [Monitor - PDF Reports](#)

### Report Groups

The set of recommended reports and grouped as 'Possible Compromise' for review and email distribution.

**Monitor > PDF Reports > Report Groups**

<input type="checkbox"/> Name	Title Page	Title	Widgets
<input checked="" type="checkbox"/> Possible Compromise	<input checked="" type="checkbox"/>	Possible Compromise	Clients sinkholed Wildfire malicious verdicts Wildfire verdicts SMTP Hosts visit malicious sites Host-visit malicious sites plus Hosts visit questionable sites Host-visit quest sites plus

**Email Scheduler**

The report group ‘Possible Compromise’ is set up to be emailed using the referenced email profile as part of the device settings.

**Monitor > PDF Reports > Email Scheduler**

Email Scheduler

Name

Possible Compromise

PDF Report or Report Group

Possible Compromise

Email Profile

Sample\_Email\_Profile

Recurrence

Disable

Override Email Addresses

Send test email

OK

Cancel

It is up to the user to finalize configuration by setting the recurrence for how often the email should be generated and sent.



---

## Config Validations: PAN-OS

---

Validation skillets allow for assessment of the config files or system state with pass/fail outputs based on validation skillet test rules. Each test result is mapped to its respective section in the Visual Guide for manual review and remediation.

The following validations are provided with IronSkillet

### 6.1 Full Configuration Assessment

*View validation test file:* [ [9.0](#) | [9.1](#) ]

Looks at a firewall xml configuration file to determine what elements recommended by IronSkillet are missing from the analyzed config file. Types of validation tests include the following based on IronSkillet recommendations:

- telemetry enabled
- dynamic updates configured
- use of snmpv3
- dns and ntp configured
- login banner configured
- timezone set to UTC
- auto acquire commit lock enabled
- X-Forward-For settings
- http range disabled
- inspection queue related settings
- max rows for CSV export
- API key lifetime
- admin attempts, timeout, and lockout

- Wildfire file size limits configured
- enable application block page
- disable log suppression
- prevent TCP evasions
- configure password complexity
- recommended zone protection profile
- inclusion of IronSkillet named profiles and groups
- logging configuration
- EDL block rules
- reference no-decrypt rules for cert checks
- address objects
- report and email scheduler related configuration

## 6.2 Upgrade to Newer Release Deltas

*View validation test file:* [ [9.0](#) | [9.1](#) ]

Looks at a firewall xml configuration file to determine what elements recommended by IronSkillet are missing from a recently upgraded PAN-OS version to 9.x. Types of validation tests include the following based on IronSkillet recommendations:

- addition of panw-bulletproof-ip-list to the EDL block rules
- API key lifetime configured
- WF file size limits for script
- IPv4 sinkhole address object is using FQDN
- default-paloalto-cloud is used for the DNS security service setting in the anti-spyware profile
- new URL categories such as newly-registered-domain, grayware and cryptocurrency have been added

---

## Default Loadable Configurations

---

The default loadable configurations have been created using the iron-skillet default and sample values. These configurations can be loaded into Panorama or a firewall for day one purposes.

**Warning:** Before committing the default configuration, be sure to edit the superuser name and password to avoid unauthorized access

---

**Note:** The values for syslog IP address, the email profile, and the config export IP address are sample information and should be updated specific to the user's environment.

---

Each directory corresponds to variations in the configuration specific to the Panorama and firewall management IP addresses:

- sample-cloud options: management interfaces for Panorama and PAN-OS use DHCP
- sample-mgmt-dhcp: PAN-OS default to DHCP while Panorama uses a static IP interface
- sample-mgmt-static: both PAN-OS and Panorama use static IP Interfaces for management

Included for each type are a set command .conf file and xml full configuration file. Both include the same configurations. Also in each directory is the config\_variables.yaml file to see what values were used to create the full configuration.

---

**Note:** Panorama can be configured using shared elements and device-specific elements. The default loadable configurations are specific to the shared model only.

---

## 7.1 SET commands

This model uses traditional CLI ‘copy-and-paste’ to load in the configuration line by line. Users can elect to edit default values for their specific deployment as each line is added or load the configuration as-is and then edit using the instructions below for *GUI variable edits* or *CLI variable edits* to the default configuration.

---

**Note:** The set command conf file includes options for standard/static or dhcp management interfaces. Only load the commands specific to the interface type to be used.

---

### Adding the configuration with set commands

- get the conf file specific to the deployment type
- log into the CLI and enter *configure* for configuration mode
- copy set commands from the .conf file and paste into the terminal

---

**Note:** It is recommended that the user only grab 30-40 set commands per paste to avoid any buffer issues resulting in errors.

---

## 7.2 XML configuration file

The full configuration file can be imported and loaded using the management GUI.

Instead of using scripting tools, the instructions below allow a user to `Import` and `Load` a candidate configuration that can be manually edited by *GUI variable edits* or *CLI variable edits*.

**Warning:** Loading a full configuration file will replace the existing candidate configuration. Save a copy of the existing configuration prior to loading the iron-skillet xml configuration file. Edit any local values before committing as a running configuration.

### 7.2.1 Import the configuration file using the GUI

1. Click on the `Device` tab
2. Select `Setup` in the left nav bar
3. Click on the `Operations` tab
4. Then `Import` named configuration snapshot choosing the day one config xml file

---

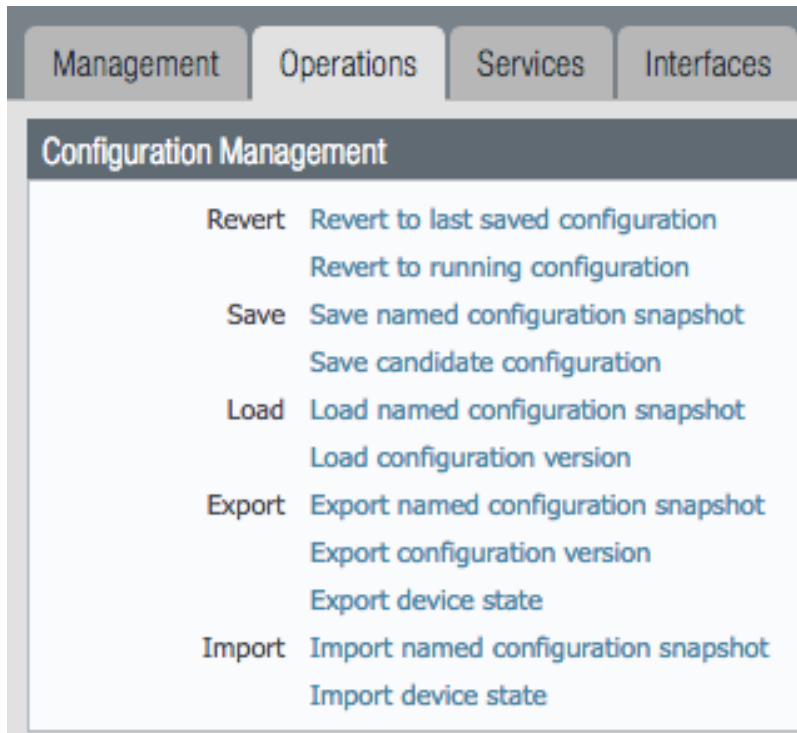
**Note:** You should perform a `Save` named configuration snapshot as backup prior to loading the new configuration

---

### 7.2.2 Load the configuration

1. Still under the `Operations` tab, use `Load` named configuration snapshot choosing the day one config xml file

2. Ensure no errors loading the configuration.



**Note:** If you see `{{ text }}` related import or load errors ensure you have the template file imported from the `loadable_configs` directory and not the `templates` directory.

## 7.3 GUI variable edits

After loading the configurations using `set` or `xml` commands, users can edit specific values instead of using the iron-skilllet defaults.

The complete list of variables used by iron-skilllet can be found at [Creating Loadable Configurations](#).

### 7.3.1 GUI variable edits: Firewall

The steps below are for a stand-alone NGFW platform without Panorama.

#### Device tab edits

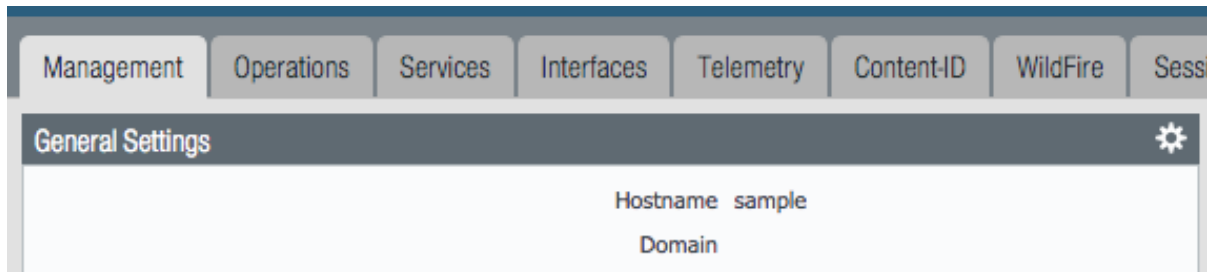
The following edits are found under the `Device` tab



From here the following edits can be made:

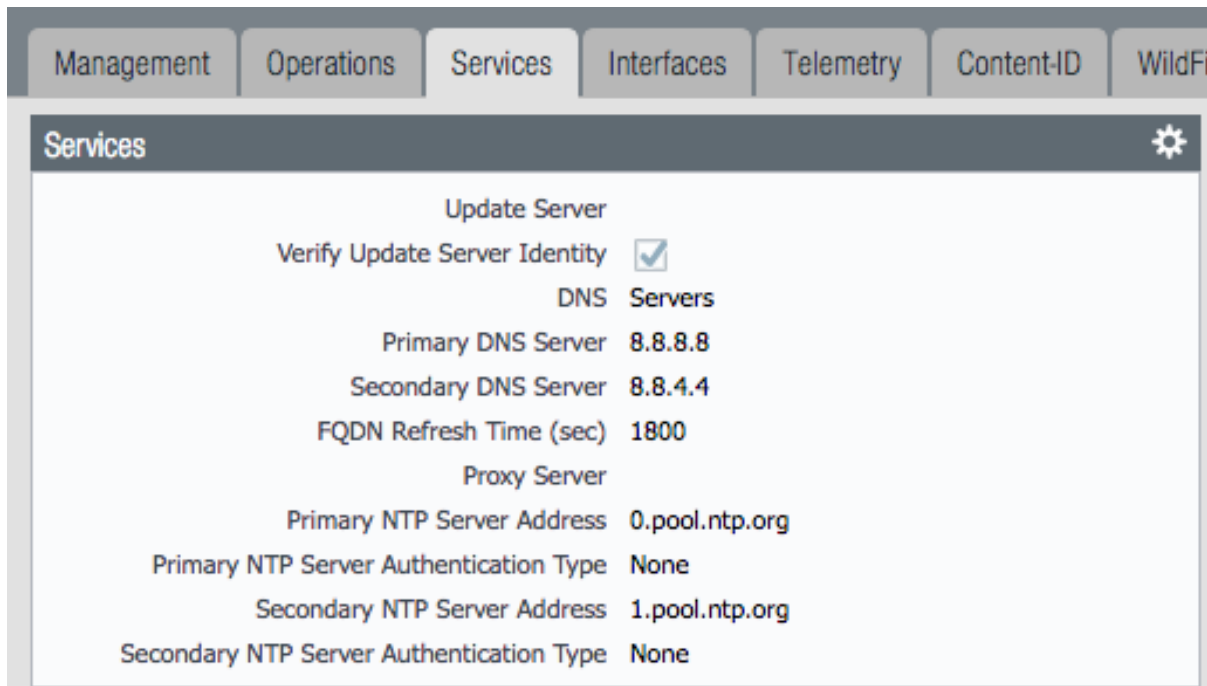
## Hostname

1. Go to Device → Setup → Management
2. Click the `gear` icon to edit the hostname



## DNS and NTP servers

1. Go to Device → Setup → Services
2. Click the `gear` icon to edit the server values
3. Choose the Services (DNS) and NTP tabs accordingly



## Static Management Interface

For a static management interface configuration, edit the IP address, subnet mask, default gateway.

1. Go to Device → Setup → Interfaces
2. Click on the `Management` link
3. Edit the management interface attributes

Management	Operations	Services	Interfaces	Telemetry	Content-ID
Interface Name		Enabled			
Management		<input checked="" type="checkbox"/>			

### Superuser Administrator

The sample configuration uses the default admin/admin username and password setting. It is recommended to remove this user and add a new superuser or at a minimum change the admin user password.

1. Go to Device → Administrators
2. Select and delete the admin user account
3. Choose to Add a new user entering the username and password in the pop-up window

<input type="checkbox"/>	Name	Role	Authentication Profile
<input checked="" type="checkbox"/>	admin	Superuser	

### Syslog IP Address

Syslog is used to send traffic, threat and other log updates to an external system.

1. Go to Device → Server Profiles → Syslog
2. Click on the Sample\_Syslog\_Profile link and edit the IP address

<input type="checkbox"/>	Name	Location	Name	Syslog Server
<input checked="" type="checkbox"/>	Sample_Syslog_Profile		Sample_Syslog	192.0.2.2

### Email Server Profile

The email profile is used to send key alerts to select recipients.

1. Go to Device → Server Profiles → Email
2. Click on the Sample\_Email\_Profile link and edit the from, to, and gateway values in the pop-up window.

<input type="checkbox"/>	Name	Servers		
		From	To	Email Gateway
<input checked="" type="checkbox"/>	Sample_Email_Profile	test@yourdomain.com	test@yourdomain.com	192.0.2.1

### Object tab edits

The following edits are found under the Objects tab

Dashboard	ACC	Monitor	Policies	Objects	Network	Device
-----------	-----	---------	----------	---------	---------	--------

From here the following edits can be made:

## Addresses

The template uses two address objects for sinkhole values, one each for IPv4 and IPv6. These are referenced in security rules.

1. Go to Objects → Address
2. Click on the Sinkhole IPv4 and IPv6 links and edit the IP address

	Name	Type	Address
<input type="checkbox"/>	<a href="#">Sinkhole-IPv4</a>	IP Netmask	72.5.65.111
<input type="checkbox"/>	<a href="#">Sinkhole-IPv6</a>	IP Netmask	2600:5200::1

## Anti-Spyware Security Profiles

The templates define multiple named Anti-Spyware profiles all appended with -AS. Each of these profiles must be updated with new sinkhole address if non-default values are required.

These values should match the sinkhole IP addresses configured under Addresses.

1. Go to Objects → Security Profiles → Anti-Spyware

<input type="checkbox"/>	Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	
<input type="checkbox"/>	<a href="#">default</a>	Predefined	Rules: 4	simple-critical	any	critical	default	disable	d
				simple-high	any	high	default	disable	
				simple-medium	any	medium	default	disable	
				simple-low	any	low	default	disable	
<input type="checkbox"/>	<a href="#">strict</a>	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable	d
				simple-high	any	high	reset-both	disable	
				simple-medium	any	medium	reset-both	disable	
				simple-informational	any	informational	default	disable	
				simple-low	any	low	default	disable	
<input type="checkbox"/>	<a href="#">Outbound-AS</a>		Rules: 2	Block-Critical-High-Medium	any	high,critical,med...	reset-both	single-packet	s
				Default-Low-Info	any	low,informational	default	disable	
<input type="checkbox"/>	<a href="#">Inbound-AS</a>		Rules: 2	Block-Critical-High-Medium	any	high,critical,med...	reset-both	single-packet	s
				Default-Low-Info	any	low,informational	default	disable	
<input type="checkbox"/>	<a href="#">Internal-AS</a>		Rules: 2	Block-Critical-High	any	high,critical	reset-both	single-packet	s
				Default-Medium-Low-Info	any	low,informationa...	default	disable	
<input type="checkbox"/>	<a href="#">Alert-Only-AS</a>		Rules: 1	Alert-All	any	any	alert	disable	d
<input type="checkbox"/>	<a href="#">Exception-AS</a>								s

2. Click on one of the template specific profiles ending in -AS
3. Click on the DNS Signatures tab and update the IPv4 and IPv6 sinkhole addresses

Anti-Spyware Profile

Name: Outbound-AS

Description:

Rules Exceptions **DNS Signatures**

External Dynamic List Domains	Action on DNS Queries
Palo Alto Networks DNS Signatures	sinkhole

+ Add - Delete

Sinkhole IPv4: 72.5.65.111

Sinkhole IPv6: 2600:5200::1

Packet Capture: single-packet

### 7.3.2 GUI variable edits: Panorama

The steps below are for edits to the Panorama configuration. Variable edits in the GUI will include both the Panorama system edits and managed firewall device-group and template configurations.

There are four areas to be edited:

- Panorama platform settings
- iron-skillet template for shared device and network items
- sample template stack for device-specific items
- Shared device-group for shared objects and policies

#### Panorama tab edits

The following edits are found under the Panorama tab

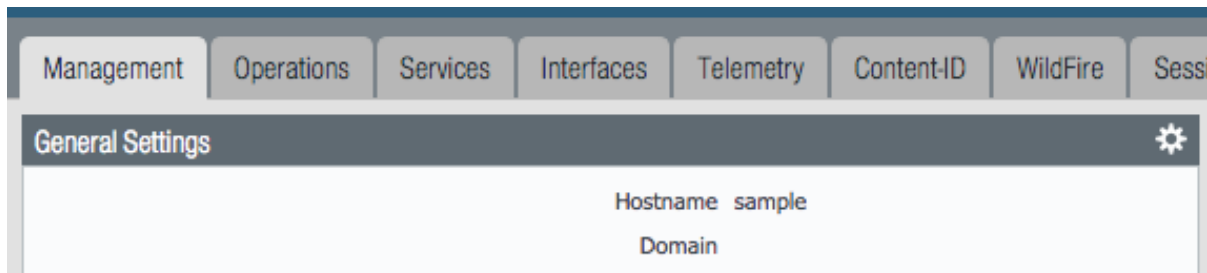


From here the following edits can be made:

#### Panorama > Hostname

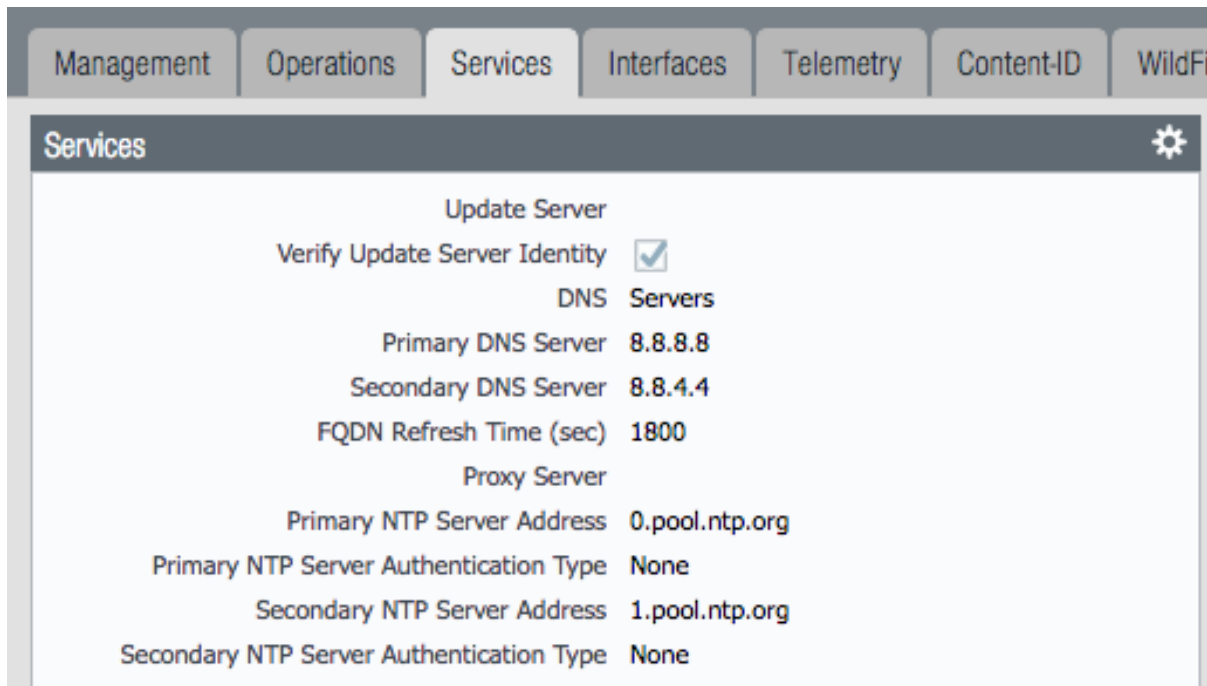
1. Go to Panorama → Setup → Management

2. Click the `gear` icon to edit the Panorama hostname



### Panorama > DNS and NTP servers

1. Go to Panorama -> Setup -> Services
2. Click the `gear` icon to edit the server values
3. Choose the Services (DNS) and NTP tabs accordingly



### Panorama > Management Interface

This configuration is specific to the Panorama management interface when statically defined.

1. Go to Panorama -> Setup -> Interfaces
2. Click on the `Management` link
3. Edit the management interface attributes

Management	Operations	Services	Interfaces	WildFire	HSM
Interface Name		IP Address			
Management		192.168.55.7			

### Panorama > Superuser Administrator

The sample configuration uses the default admin/admin username and password setting. It is recommended to remove this user and add a new superuser or at a minimum change the admin user password.

1. Go to Panorama → Administrators
2. Select and delete the admin user account
3. Choose to Add a new user entering the username and password in the pop-up window

<input type="checkbox"/>	Name	Role	Authentication Profile
<input checked="" type="checkbox"/>	admin	Superuser	

### Panorama > Syslog IP Address

Syslog is used to send traffic, threat and other log updates to an external system.

1. Go to Panorama → Server Profiles → Syslog
2. Click on the Sample\_Syslog\_Profile link and edit the IP address

<input type="checkbox"/>	Name	Location	Name	Syslog Server
<input checked="" type="checkbox"/>	Sample_Syslog_Profile		Sample_Syslog	192.0.2.2

### Panorama > Email Server Profile

The email profile is used to send key alerts to select recipients.

1. Go to Panorama → Server Profiles → Email
2. Click on the Sample\_Email\_Profile link and edit the from, to, and gateway values in the pop-up window.

<input type="checkbox"/>	Name	Servers		
		From	To	Email Gateway
<input checked="" type="checkbox"/>	Sample_Email_Profile	test@yourdomain.com	test@yourdomain.com	192.0.2.1

### Panorama > Config Bundle Export Server

1. Go to Panorama → Scheduled Config Export

2. Click on the Recommended\_Config\_Export link
3. In the pop-up window, edit the Hostname value

The screenshot shows a web interface with a sidebar on the left containing two items: 'Name' (unchecked) and 'Recommended\_Config\_Export' (checked). The main area displays a 'Scheduled Config Export' dialog box. The dialog has a title bar with a question mark icon. Inside, the 'Name' field is set to 'Recommended\_Config\_Export'. The 'Description' field is empty. The 'Enable' checkbox is checked. The 'Scheduled Export Start Time (Daily)' is set to '02:00' with a dropdown arrow and a range of '00:00 - 23:59'. The 'Protocol' is set to 'SCP' with radio buttons for 'SCP' and 'FTP'. The 'Hostname' is '192.0.2.3', 'Port' is '[1 - 65535]', and 'Path' is empty. The 'Username' is 'testuser', 'Password' is masked with dots, and 'Confirm Password' is also masked. At the bottom, there are three buttons: 'Test SCP server connection', 'OK', and 'Cancel'.

### Panorama > Template Stack

1. Go to Panorama -> Template
2. Click on the sample\_stack link and edit the name

### Panorama > Device-Group

1. Go to Panorama → Device-Groups
2. Click on the `sample_devicegroup` link and edit the name

### Templates > Device tab edits

The following edits are found under the Device tab




---

**Note:** The edits are grouped by the *iron-skillet* template edits and *sample\_stack* template stack edits

---

\*\* iron-skillet template edits\*\*

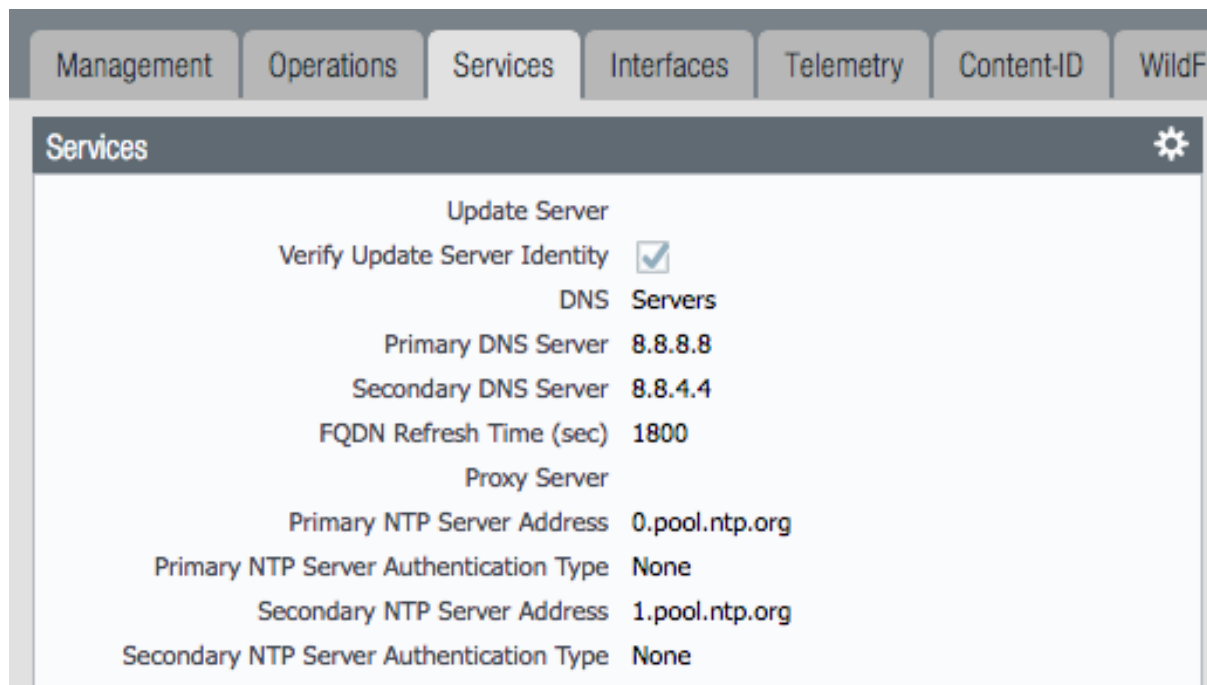
---

**Note:** Make sure the template selected in the GUI is *iron-skillet* before completing the steps below

---

### DNS and NTP servers

1. Go to Device → Setup → Services
2. Click the gear icon to edit the server values
3. Choose the Services (DNS) and NTP tabs accordingly



Management Operations **Services** Interfaces Telemetry Content-ID WildFire

**Services** ⚙️

Update Server

Verify Update Server Identity ☒

DNS Servers

Primary DNS Server 8.8.8.8

Secondary DNS Server 8.8.4.4

FQDN Refresh Time (sec) 1800

Proxy Server

Primary NTP Server Address 0.pool.ntp.org

Primary NTP Server Authentication Type None

Secondary NTP Server Address 1.pool.ntp.org

Secondary NTP Server Authentication Type None

### Superuser Administrator

The sample configuration uses the default admin/admin username and password setting. It is recommended to remove this user and add a new superuser or at a minimum change the admin user password.

1. Go to Device → Administrators
2. Select and delete the `admin` user account
3. Choose to Add a new user entering the username and password in the pop-up window

<input type="checkbox"/>	Name	Role	Authentication Profile
<input checked="" type="checkbox"/>	admin	Superuser	

### Syslog IP Address

Syslog is used to send traffic, threat and other log updates to an external system.

1. Go to Device → Server Profiles → Syslog
2. Click on the `Sample_Syslog_Profile` link and edit the IP address

<input type="checkbox"/>	Name	Location	Name	Syslog Server
<input type="checkbox"/>	<a href="#">Sample_Syslog_Profile</a>		Sample_Syslog	192.0.2.2

### Email Server Profile

The email profile is used to send key alerts to select recipients.

1. Go to Device → Server Profiles → Email

- Click on the `Sample_Email_Profile` link and edit the from, to, and gateway values in the pop-up window.

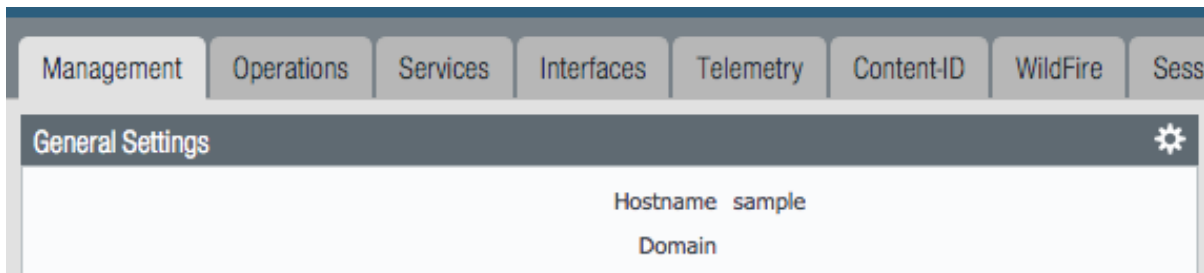
		Servers	
<input type="checkbox"/> Name	From	To	Email Gateway
<input type="checkbox"/> <a href="#">Sample_Email_Profile</a>	test@yourdomain.com	test@yourdomain.com	192.0.2.1

\*\* iron-skillet template edits\*\*

**Note:** Make sure the template selected in the GUI is *sample\_stack* (or the updated name) before completing the steps below

### Hostname

- Go to Device → Setup → Management
- Click the gear icon to edit the hostname



### Static Management Interface

For a static management interface configuration, edit the IP address, subnet mask, default gateway.

- Go to Device → Setup → Interfaces
- Click on the `Management` link
- Edit the management interface attributes

Management	Operations	Services	Interfaces	Telemetry	Content-ID
Interface Name		Enabled			
<a href="#">Management</a>		<input checked="" type="checkbox"/>			

\*\* Shared device-group edits\*\*

**Note:** Make sure the device-group selected in the GUI is *Shared* before completing the steps below

### Device-Group > Objects tab edits

The following edits are found under the `Objects` tab



From here the following edits can be made:

### Addresses

The template uses two address objects for sinkhole values, one each for IPv4 and IPv6. These are referenced in security rules.

1. Go to Objects → Address
2. Click on the Sinkhole IPv4 and IPv6 links and edit the IP address

	Name	Type	Address
<input type="checkbox"/>	Sinkhole-IPv4	IP Netmask	72.5.65.111
<input type="checkbox"/>	Sinkhole-IPv6	IP Netmask	2600:5200::1

### Anti-Spyware Security Profiles

The templates define multiple named Anti-Spyware profiles all appended with -AS. Each of these profiles must be updated with new sinkhole address if non-default values are required.

These values should match the sinkhole IP addresses configured under Addresses.

1. Go to Objects → Security Profiles → Anti-Spyware

<input type="checkbox"/>	Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	D
<input type="checkbox"/>	default	Predefined	Rules: 4	simple-critical	any	critical	default	disable	d
				simple-high	any	high	default	disable	
				simple-medium	any	medium	default	disable	
				simple-low	any	low	default	disable	
<input type="checkbox"/>	strict	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable	d
				simple-high	any	high	reset-both	disable	
				simple-medium	any	medium	reset-both	disable	
				simple-informational	any	informational	default	disable	
				simple-low	any	low	default	disable	
<input type="checkbox"/>	Outbound-AS		Rules: 2	Block-Critical-High-Medium	any	high,critical,med...	reset-both	single-packet	s
				Default-Low-Info	any	low,informational	default	disable	
<input type="checkbox"/>	Inbound-AS		Rules: 2	Block-Critical-High-Medium	any	high,critical,med...	reset-both	single-packet	s
				Default-Low-Info	any	low,informational	default	disable	
<input type="checkbox"/>	Internal-AS		Rules: 2	Block-Critical-High	any	high,critical	reset-both	single-packet	s
				Default-Medium-Low-Info	any	low,informationa...	default	disable	
<input type="checkbox"/>	Alert-Only-AS		Rules: 1	Alert-All	any	any	alert	disable	d
<input type="checkbox"/>	Exception-AS								s

2. Click on one of the template specific profiles ending in -AS
3. Click on the DNS Signatures tab and update the IPv4 and IPv6 sinkhole addresses

**Anti-Spyware Profile**

Name: Outbound-AS

Description:

Rules | Exceptions | **DNS Signatures**

External Dynamic List Domains	Action on DNS Queries
Palo Alto Networks DNS Signatures	sinkhole

+ Add - Delete

Sinkhole IPv4: 72.5.65.111

Sinkhole IPv6: 2600:5200::1

Packet Capture: single-packet

## 7.4 CLI variable edits

After loading the configurations using `set` or `xml` commands, users can edit specific values instead of using the iron-skillet defaults.

The complete list of variables used by iron-skillet can be found at [Creating Loadable Configurations](#).

### 7.4.1 CLI variable edits: Firewall

This section is specific to a non-Panorama managed NGFW.

Instead of using the GUI to make template edits for each variable value, below are steps using SET commands to make the same candidate configuration changes.

The `{{ text }}` values denotes where a variable is used in the template.

#### Hostname

```
set deviceconfig system hostname {{ hostname }}
```

#### DNS and NTP Servers

```
set deviceconfig system dns-setting servers primary {{ DNS 1 }} secondary {{ DNS 2 }}
set deviceconfig system ntp-servers primary-ntp-server ntp-server-address {{ NTP 1 }}
set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address {{ NTP 2 }}
↩ }
```

(continues on next page)

(continued from previous page)

---

### Static management interface

```
set deviceconfig system ip-address {{ ip address }} netmask {{ mask }} default-  
↳gateway {{ gateway }}
```

### Superuser admin account

```
set mgt-config users {{ username }} permissions role-based superuser yes  
set mgt-config users {{ username }} password
```

When the password command is entered, the user will be prompted for a password.

### Syslog and Email Server Profiles

```
set shared log-settings syslog Sample_Syslog_Profile server Sample_Syslog server {{  
↳ip address }}  
set shared log-settings email Sample_Email_Profile server Sample_Email_Profile from {  
↳{ from }}  
set shared log-settings email Sample_Email_Profile server Sample_Email_Profile to {{  
↳to }}  
set shared log-settings email Sample_Email_Profile server Sample_Email_Profile_  
↳gateway {{ address }}
```

### Address Objects

```
set address Sinkhole-IPv4 ip-netmask {{ IPv4 address }}  
set address Sinkhole-IPv6 ip-netmask {{ IPv6 address }}
```

### Anti-Spyware Security Profiles

The same commands are used across all of the template security profiles ending in -AS.

```
set profiles spyware {{ profile name }} botnet-domains sinkhole ipv4-address {{ IPv4_  
↳address }}  
set profiles spyware {{ profile name }} botnet-domains sinkhole ipv6-address {{ IPv6_  
↳address }}
```

---

## 7.4.2 CLI variable edits: Panorama

This section is specific to configuration of a Panorama management system.

Instead of using the GUI to make template edits for each variable value, below are steps using SET commands to make the same candidate configuration changes.

The {{ text }} values denotes where a variable is used in the template.

---

**Note:** The initial configurations are specific to the Panorama platform itself. The managed firewall configurations are added under the template and device-group configurations.

---

### Panorama > Hostname

```
set deviceconfig system hostname {{ hostname }}
```

### Panorama > DNS and NTP Servers

```
set deviceconfig system dns-setting servers primary {{ DNS 1 }} secondary {{ DNS 2 }}
set deviceconfig system ntp-servers primary-ntp-server ntp-server-address {{ NTP 1 }}
set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address {{ NTP 2 }}
↵
```

### Panorama > Static management interface

```
set deviceconfig system ip-address {{ ip address }} netmask {{ mask }} default-
↵gateway {{ gateway }}
```

### Panorama > Superuser admin account

```
set mgt-config users {{ username }} permissions role-based superuser yes
set mgt-config users {{ username }} password
```

When the password command is entered, the user will be prompted for a password.

### Panorama > Syslog and Email Server Profiles

```
set panorama log-settings syslog Sample_Syslog_Profile server Sample_Syslog server {{
↵ip address }}
set panorama log-settings email Sample_Email_Profile server Sample_Email_Profile from
↵{{ from }}
set panorama log-settings email Sample_Email_Profile server Sample_Email_Profile to {
↵{ to }}
set panorama log-settings email Sample_Email_Profile server Sample_Email_Profile
↵gateway {{ address }}
```

### Panorama > Config Bundle Export Schedule

```
set deviceconfig system config-bundle-export-schedule Recommended_Config_Export
↵protocol scp hostname {{ ip address }}
```

---

**Note:** The configuration for Panorama has some element in the iron-s skillet shared template and others specific to the device captured as a template-stack called `sample_stack`. The same is true for device-group items that are either shared or contained in a device-specific group, namely reports.

---

### Template > Hostname

```
set template-stack sample_stack config deviceconfig system hostname {{ hostname }}
```

### Template > DNS and NTP Servers

```
set template iron-s skillet config deviceconfig system dns-setting servers primary {{
↵DNS 1 }} secondary {{ DNS 2 }}
set template iron-s skillet config deviceconfig system ntp-servers primary-ntp-server
↵ntp-server-address {{ NTP 1 }}
set template iron-s skillet config deviceconfig system ntp-servers secondary-ntp-server
↵ntp-server-address {{ NTP 2 }}
```

**Template > Static management interface**

This is to be configured for a firewall with a static management interface.

```
set template-stack sample_stack config deviceconfig system ip-address {{ ip address }}
set template-stack sample_stack config deviceconfig system netmask {{ mask }}
set template-stack sample_stack config deviceconfig system default-gateway {{ gateway_
↪ }}
```

**Template > Superuser admin account**

```
set template iron-skillet config mgt-config users {{ username }} permissions role-
↪based superuser yes
set template iron-skillet config mgt-config users {{ username }} password
```

When the password command is entered, the user will be prompted for a password.

**Template > Syslog and Email Server Profiles**

```
set template iron-skillet config shared log-settings syslog Sample_Syslog_Profile_
↪server Sample_Syslog server {{ ip address }}
set template iron-skillet config shared log-settings email Sample_Email_Profile_
↪server Sample_Email_Profile from {{ from }}
set template iron-skillet config shared log-settings email Sample_Email_Profile_
↪server Sample_Email_Profile to {{ to }}
set template iron-skillet config shared log-settings email Sample_Email_Profile_
↪server Sample_Email_Profile gateway {{ address }}
```

**Device-Group > Address Objects**

```
set shared address Sinkhole-IPv4 ip-netmask {{ IPv4 address }}
set shared address Sinkhole-IPv6 ip-netmask {{ IPv6 address }}
```

**Device-Group Anti-Spyware Security Profiles**

The same commands are used across all of the templated security profiles ending in -AS.

```
set shared profiles spyware {{ profile name }} botnet-domains sinkhole ipv4-address {
↪{ IPv4 address }}
set shared sample profiles spyware {{ profile name }} botnet-domains sinkhole ipv6-
↪address {{ IPv6 address }}
```

---

### Formula-based Excel Spreadsheet

---

For users who want to customize their configuration before loading without the use of python utilities, this is a preferred model for configuration.

The spreadsheets can be found at:

*PAN-OS* [ 8.0 | 8.1 | 9.0 ]

*Panorama* [ 8.0 | 8.1 | 9.0 ]

The `values` worksheet can be updated with user-specific values. Formulas embedded in the `set` commands worksheet will use the user added values.

Once the spreadsheet is updated, the traditional copy-and-paste model can be used to load the configuration using the CLI.

**Warning:** The set commands use formulas referencing cells in the values worksheet. Use caution if making changes to the base spreadsheet to avoid incorrect references to cell values.



---

# Creating Loadable Configurations

---

The base templates are designed for variable substitution. The variables provide flexibility for templates configurations to be modified specific to each deployment.

A jinja model for variables is used with the form `{{ variable }}`

**Warning:** The configuration templates for device and Panorama system include jinja ‘if’ conditionals. These are used by the `create_loadable_configs.py` tool to determine what IP information should be added regarding the management interface.

If the tool or jinja formats will not be used, remove the `{% text %}` statements. The user will also have to manually replace the variables in order for the config to load and commit

## 9.1 Variables list and descriptions

The table below lists the template variables along with placeholder or recommended settings.

Variable name	Default value	Description
ADMINISTRATOR_USERNAME	admin	superuser id; prompted when using build_my_config tool
ADMINISTRATOR_PASSWORD	admin [change first]	superuser password; prompted and hashed in build_my_config
FW_NAME	sample	used for hostname and device-group/template in Panorama
STACK	sample_stack	Panorama sample template name
DEVICE_GROUP	sample_devicegroup	Panorama sample device-group name
DNS_1	8.8.8.8 (Google)	primary DNS server
DNS_2	8.8.4.4 (Google)	secondary DNS server
NTP_1	0.pool.ntp.org	primary NTP server
NTP_2	1.pool.ntp.org	secondary NTP server
SINKHOLE_IPV4	72.5.65.111	IPv4 sinkhole address (Palo Alto Networks)
SINKHOLE_IPV6	2600:5200::1	IPv6 sinkhole address (IPv6 bogon)
EMAIL_PROFILE_GATEWAY	192.0.2.1	email profile gateway address; NET-1 default
EMAIL_PROFILE_FROM	sent-from@yourdomain.com	from address for email alerts
EMAIL_PROFILE_TO	sendto@yourdomain.com	to address for email alerts
SYSLOG_SERVER	192.0.2.2	syslog IP address; NET-1 unroutable default
CONFIG_EXPORT_IP	192.0.2.3	config bundle export target from Panorama; NET-1 default
MGMT_TYPE	dhcp-client	Firewall mgmt IP type (dhcp-client or static)
MGMT_IP	192.168.55.10	Firewall mgmt IP if type=static
MGMT_MASK	255.255.255.0	Firewall netmask if type=static
MGMT_DG	192.168.55.2	Firewall default gateway if type=static
CONFIG_PANORAMA_IP	yes	For build_my_config, determine if Panorama IP to be added
PANORAMA_TYPE	standard	Used in order to set mgmt interface for standard or cloud
PANORAMA_IP	192.168.55.7	Panorama IP if to be added to my_config
PANORAMA_MASK	255.255.255.0	Panorama netmask if to be added to my_config
PANORAMA_DG	192.168.55.2	Panorama default gateway if to be added to my_config
API_KEY_LIFETIME	525600	Panorama and device API key lifetime in minutes
INCLUDE_PAN_EDL	yes	Include the panw edl object security rules

## 9.2 Create Loadable Configuration python utility

The tools folder in the iron-skillet repo contains a simple python utility for variable substitution.

This tools folder can be found at:

*Release branch* [ 8.0 | 8.1 | 9.0 ]

The directions below detail how to use the utility in a python virtual environment on Mac or Linux. Similar instructions can work for Windows with python and pip installed.

---

**Note:** This tool is designed for Python 3.6 or layer.

---

---

**Note:** The examples below show PAN-OS 9.0 and other releases can be used by changing the release/branch version.

---

## 9.2.1 Install the repo and tools

The initial step is to clone the repo to a local machine with release/branch panos\_v9.0.

Clone using ssh:

```
$ git clone -b panos_v9.0 git@github.com:PaloAltoNetworks/iron-skillet.git
```

Clone using https:

```
$ git clone -b panos_v9.0 https://github.com/PaloAltoNetworks/iron-skillet.git
```

After the repo is cloned locally, the following steps are used to setup and activate the python virtual environment.

---

**Note:** The example below shows python version 3.6 in the second step. If using python 3.5 or 3.7, replace with the respective version

---

```
$ cd iron-skillet/tools
$ python3.6 -m venv env
$ source env/bin/activate
(env)$ pip install -r requirements.txt
```

The virtual environment name is `env` and if active will likely be shown to the left of the command prompt. If successful, the iron-skillet templates and tools are now ready to use.

## 9.2.2 Update the variable values

Inside the tools directory, update the `config_variables.yaml` file then run `create_loadable_configs.py`. The example shows the `vi` text editor but any text editor may be used.

```
(env)$ cd iron-skillet/tools [if not in the tools directory]
(env)$ vi config_variables.yaml
```

Edit the `config_variables.yaml` file for your local deployment and save.

Key variables to edit include:

- management interface type: static or dhcp-client based on firewall deployment
- Panorama deployment type: standard or cloud based on Panorama deployment

## 9.2.3 Run the application

Ensure the variable values are correct and run the application.

```
(env)$ python3 create_loadable_configs.py
>>> Enter the name of the output directory:
>>> Enter the superuser administrator account username:
>>> Enter the superuser administrator account password:
```

This will run the python utility and output set commands and full xml config files. Loadable configs are stored in the loadable\_configs directory. The config folder prefix is based on the output directory name used when running the script.

**Warning:** You will be prompted for a username/password that will be used in the configuration file. A hash is created for the password so it is unreadable and the default admin/admin is removed. Remember the user/password information before committing to a running firewall or Panorama.

---

### Loading the XML templates

---

The template are xml file format that have to be loaded into the device as a full config or with modular partial loading. Multiple options including GUI, CLI, and API can be utilized. The sections below give details for template loading using various models specific to the users expertise and current operational environment.

---

**Note:** Sample configuration files are in the `loadable_configs` directory. Samples include a static management interface, basic dhcp-client management interface, and additional dhcp-client options for cloud deployments. These configurations are loadable and can be manually edited although user-specific configurations can be created using the ``create_loadable_configs`` utility in the tools folder.

---

#### 10.1 Preparing the configuration files

---

The template files in the `panos` and `panorama` directories are xml format. These templates are using a jinja variable model in the xml as `{{ variable name }}`. In order to have a loadable configuration, the recommended practice is to use `create_loadable_configs.py` in the tools folder.

The *Creating Loadable Configurations* documentation section details how to use this tool.

The output of the tool will be a set of xml snippet and full configuration files stored in the `loadable_configs` folder.

#### 10.2 Load full configuration file

---

Either at the time of VM instantiation or post deploy, a full xml can be loaded into the system as a candidate configuration. This provides the simplicity of loading a new configuration but will replace any configuration currently in the device.

In comparison, a load config partial requires additional steps but merges into the existing configuration instead of replacing.

The steps below are for for a full configuration load and replace.

### 10.2.1 Edit the full xml configuration file

Since this will replace the existing configuration, the user is required to modify the xml file with admin accounts, management IP, and other initial configuration values. The template uses `{{ text }}` markers in the config file to denote values that MUST be changed.

**Warning:** During a commit, the device will show an error with the variable `{{ text }}` values in the error message. These values must be modified offline and the file imported for a successful load and commit.

---

**Note:** The user is recommended to use the `create_loadable_configs.py` tool to have a loadable configuration file

---

### 10.2.2 Import the configuration file using the GUI

1. Log into the firewall and click on the `Device` tab
2. Select `Setup` in the left nav bar
3. Click on the `Operations` tab
4. Then `Import` named `configuration snapshot` choosing the day one config xml file

---

**Note:** You should perform a `Save` named `configuration snapshot` as backup prior to loading the new configuration

---

### 10.2.3 Load and commit the configuration

1. Still under the `Operations` tab, use `Load` named `configuration snapshot` choosing the day one config xml file
2. Ensure no errors loading the configuration.
3. Once loaded use the GUI to verify the configuration elements have been loaded then `commit`

---

**Note:** As referenced above, you may see `{{ text }}` related errors during the commit. If this happens, you will need to edit the pre-imported xml file and then repeat the steps above to import, load, and commit the configuration.

---

## 10.3 Using Load Config Partial

---

The configuration file uses the xml format. Therefore each configuration element sits in the xml tree and is referenced by its `xpath`.

Using this concept, a template configuration file can be imported into Panorama or the firewall with only the referenced elements merged into the existing configuration. This is more modular than loading a full configuration file that replaces the existing configuration.

The syntax used for loading the templates is:

```
load config partial from {{filename}} from-xpath {{xpath}} to-xpath {{xpath}} mode merge
```

where:

`{{filename}}` is the xml file loaded into the device

`{{xpath}}` denotes what part of the configuration is being merged from the day one file to the candidate configuration.

### 10.3.1 Edit the configuration xml file

Since this will replace the existing configuration, the user is required to modify the xml file with admin accounts, management IP, and other initial configuration values. The template uses `{{ text }}` markers in the config file to denote values that MUST be changed.

**Warning:** During a commit, the device will show an error with the variable `{{ text }}` values in the error message. These values must be modified offline and the file imported for a successful load and commit.

---

**Note:** The user is recommended to use the `create_loadable_configs.py` tool to have a loadable configuration file

---

### 10.3.2 Import the Day One configuration: GUI

1. Log into the firewall and click on the `Device` tab
2. Select `Setup` in the left nav bar
3. Click on the `Operations` tab
4. Then `Import` named `configuration snapshot` choosing the day one config xml file

---

**Note:** You can perform a `Save` named `configuration snapshot` as backup prior to loading the new configuration

---

### 10.3.3 Load the configuration elements: CLI

1. Log into the PAN-OS command line interface
2. Enter `configure` to go into configuration mode
3. Paste in each of the `load config partial` commands, in order
4. Once complete use the GUI to verify the configuration elements have been loaded then `commit`

### 10.3.4 PAN-OS load config partial commands

Cut-and-paste from the table below into the PAN-OS command line while in configuration mode.

You can paste multiple items. The system will pause during each load config partial, return a status message, then move to the next load. When complete, ensure the final load is entered and a status message received.

#### *PAN-OS 8.x*

```
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→shared/log-settings to-xpath /config/shared/log-settings mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/  
→tag to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/  
→entry[@name='vsys1']/tag mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/deviceconfig/system to-xpath_  
→/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system_  
→mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/deviceconfig/setting to-xpath_  
→/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting_  
→mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/  
→address to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/  
→entry[@name='vsys1']/address mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/  
→external-list to-xpath /config/devices/entry[@name='localhost.localdomain']/  
→vsys/entry[@name='vsys1']/external-list mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/  
→profiles to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/  
→entry[@name='vsys1']/profiles mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/  
→profile-group to-xpath /config/devices/entry[@name='localhost.localdomain']/  
→vsys/entry[@name='vsys1']/profile-group mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/  
→rulebase to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/  
→entry[@name='vsys1']/rulebase mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/network/profiles/zone-  
→protection-profile to-xpath /config/devices/entry[@name='localhost.  
→localdomain']/network/profiles/zone-protection-profile mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→shared/reports to-xpath /config/shared/reports mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→shared/report-group to-xpath /config/shared/report-group mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→shared/email-scheduler to-xpath /config/shared/email-scheduler mode merge
```

#### *PAN-OS 9.0*

```

load config partial from-xpath /config/shared/log-settings to-xpath /config/
↳shared/log-settings mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/tag to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/tag mode
↳merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/deviceconfig/system to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/deviceconfig/system mode merge from
↳iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/deviceconfig/setting to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/deviceconfig/setting mode merge from
↳iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/address to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address mode
↳merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/external-list to-xpath /config/
↳devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
↳external-list mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/profiles to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/profiles
↳mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/profile-group to-xpath /config/
↳devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
↳profile-group mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/rulebase to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase
↳mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/network/profiles/zone-protection-profile to-xpath /config/
↳devices/entry[@name='localhost.localdomain']/network/profiles/zone-
↳protection-profile mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/shared/reports to-xpath /config/shared/
↳reports mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/shared/report-group to-xpath /config/
↳shared/report-group mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/shared/email-scheduler to-xpath /
↳config/shared/email-scheduler mode merge from iron_skillet_panos_full.xml

```

---

**Note:** The filename is specific to the iron-skillet templates but can be renamed if the base file is renamed. Simply use a text editor to replace the template filename with the update name.

---



---

**Note:** For subsequent updates, specific load config partial commands can be used.

---

### 10.3.5 PAN-OS config elements used in load config partial

Each xpath in the load config partial gives an indication of each element loaded. Below is a simple explanation of the configuration elements with key items in the xml load.

xpath	suffix description
log settings	settings syslog/email profiles and system, configuration logging
tag	referenced tags used in security rules
system	dynamic updates, dns and ntp server settings
setting	Wildfire max file sizes, disable log suppression
address	named references for sinkholes values used in security rules
external list	EDLs referenced in security rules, eg. IPv4/v6 bogons
profiles	Threat, URL Filtering, Wildfire, and decryption profile configurations
profile-group	Group settings for the security profiles, eg. Inbound, Outbound, Alert-All
rulebase	template security and decryption rules
zone protection	recommended zone protection profile
reports	traffic and threat reports
report groups	grouping of reports for viewing and scheduling
email scheduler	email schedule for report groups

### 10.3.6 Panorama load config partial commands

Cut-and-paste from the table below into the PAN-OS command line while in configuration mode.

You can paste multiple items. The system will pause during each load config partial, return a status message, then move to the next load. When complete, ensure the final load is entered and a status message received.

#### *Panorama 8.x*

```
load config partial from iron_skillet_panorama_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/deviceconfig/system to-xpath_  
→/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system_  
→mode merge  
load config partial from iron_skillet_panorama_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/deviceconfig/setting to-xpath_  
→/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting_  
→mode merge  
load config partial from iron_skillet_panorama_full.xml from-xpath /config/  
→panorama/log-settings to-xpath /config/panorama/log-settings mode merge  
load config partial from iron_skillet_panorama_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/template to-xpath /config/  
→devices/entry[@name='localhost.localdomain']/template mode merge  
load config partial from iron_skillet_panorama_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/device-group to-xpath /config/  
→devices/entry[@name='localhost.localdomain']/device-group mode merge  
load config partial from iron_skillet_panorama_full.xml from-xpath /config/  
→shared to-xpath /config/shared mode merge  
load config partial from iron_skillet_panorama_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/log-collector-group to-xpath_  
→/config/devices/entry[@name='localhost.localdomain']/log-collector-group_  
→mode merge
```

#### *Panorama 9.0*

```
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/deviceconfig/system to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/deviceconfig/system mode merge from_
↳iron_skillet_panorama_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/deviceconfig/setting to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/deviceconfig/setting mode merge from_
↳iron_skillet_panorama_full.xml
load config partial from-xpath /config/panorama/log-settings to-xpath /config/
↳panorama/log-settings mode merge from iron_skillet_panorama_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/template to-xpath /config/devices/entry[@name='localhost.
↳localdomain']/template mode merge from iron_skillet_panorama_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/device-group to-xpath /config/devices/entry[@name='localhost.
↳localdomain']/device-group mode merge from iron_skillet_panorama_full.xml
load config partial from-xpath /config/shared to-xpath /config/shared mode_
↳merge from iron_skillet_panorama_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/log-collector-group to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/log-collector-group mode merge from_
↳iron_skillet_panorama_full.xml
```

---

**Note:** The filename is specific to the iron-skillet templates but can be renamed if the base file is renamed. Simply use a text editor to replace the template filename with the update name.

---



---

**Note:** For subsequent updates, specific load config partial commands can be used.

---

### 10.3.7 Panorama config elements used in load config partial

Each xpath in the load config partial gives an indication of each element loaded. Below is a simple explanation of the configuration elements with key items in the xml load.

This uses an aggregate template loading module with multiple configuration elements contained under the template, device-group, and shared parts of the xml tree. The hierarchical nature of Panorama simplifies the configuration loading.

xpath	suffix description
panorama system	panorama specific dynamic updates, dns and ntp server settings
panorama settings	enable reporting on groups and sharing of unused objects
panorama log settings	syslog/email profiles and system, configuration logging
template	test template configuration with device settings and zone profile
device-group	reports, report groups, and email scheduler
shared	profile object, rules, and other device-group 'top of tree' items
log collector	settings for Panorama when used as a log collector

## 10.4 Loading Configuration Snippets using Panhandler

### 10.4.1 panHandler overview

Panhandler is container-based UI used to aggregate and load configuration templates. PanHandler simplifies input of user data and using the NGFW API to push configuration snippets.

### 10.4.2 installing and using PanHandler

PanHandler is an easily distributed and loadable Docker container. Instructions for using PanHandler can be reviewing the [PanHandler Docs](#)

## 10.5 Loading Configuration Snippets using skilletCLI

---

### 10.5.1 SkilletCLI overview

This open-source utility provides a command line interface to Palo Alto “skillets”, curated configuration templates designed to be imported into firewalls or Panorama.

### 10.5.2 installing and using SkilletCLI

Usage information for SkilletCLI is found in the repo [SkilletCLI](#)

## 10.6 Loading Configuration Snippets with Pan-Python

---

### 10.6.1 pan-python overview

Pan-python provides a simple command-line model to use the Panorama/PAN-OS API. It leverages the standard xml xpath+element model to push configuration changes to the device. The GitHub repo is found here:

[pan-python repo](#)

Training for pan-python including the initial install and getting the device api-key are found here:

[pan-python api lab](#)

Before using pan-python, it helps to be familiar with the xpaths used in the template along with the configuration load order. These provide the foundation for the xpath and element references in the examples below.

[xpath and snippet load order](#)

### 10.6.2 pan-python full syntax for loading a config element

The standard entry model is

```
panxapi.py -h {{ ip address }} -K {{ api-key }} -S {{ filename.xml }} "{{ xpath }}"
```

where the elements are:

```
{{ ip address }} is the device ip address
{{ api-key }} is the user/device specific api-key
{{ filename }} is the xml snippet to be loaded
{{ xpath }} is the xpath specific to the config element
```

For example, to load the tag.xml file to ip address 192.168.55.10 and api-key: 12345 would be

```
panxapi.py -h 192.168.55.10 -K 12345 -S tag.xml "/config/devices/entry[@name=
↪'localhost.localdomain']/vsys/entry[@name='vsys1']/tag"
```

or an external list object (aka EDL)

```
panxapi.py -h 192.168.55.10 -K 12345 -S external_list.xml "/config/devices/
↪entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/external-list"
```

Simple scripts can be used to iterate through multiple load requests.

**Note:** Based on the local pan-python install and use of .panrc you may not require the -h and -K elements and only have to reference the xpath and filename.

**Warning:** Before loading configurations, use the create\_loadable\_configs.py tool to create loadable configuration snippets. The templates have {{ variable }} elements that must be replaced.

## 10.7 The Panorama/PAN-OS API and XML

### 10.7.1 API Overview

For extended reading about the API, you can access the documentation for 8.1 here:

[PAN-OS API Reference](#)

Additional information can be found as part of the pan-python documentation:

[pan-python api lab](#)

The configuration file and api calls are XML specific. XML is based on XML nodes with the xpath specifying the node in the tree to be referenced. Thus in order to use the API, two configuration items are needed:

1. The xpath pointing to the node to be configured
2. The xml snippet to be used as the element in the configuration

Along with these two items, the IP address of the device and a user-based API are required to modify the configuration.

**Note:** Each *snippets* directory in templates contains a .meta-cnc.yaml file that includes xpath and related file names



---

## VM-50 Security Profile Limits

---

IronSkillet includes a broad set of security profiles to simplify the usage in security policies. However, the VM-50 limits the number of security profiles that can be configured to 38 resulting in possible commit errors if this limit is exceeded.

---

**Note:** If > 49 profiles, the user may see an error message that the number of profiles (39) exceeds capacity (38). This is an error in the message output and the user will have to remove enough profiles for the 38 count limit.

---

---

**Note:** Make sure the firewall is licensed. An unlicensed firewall will allow only 20 profiles, far below what is configured with IronSkillet.

---

The *delete* commands below can be used to delete security profiles and profile groups from an IronSkillet template load that may not be required for a basic VM-50 configuration yet allow for a reduced number of profiles.

Copy/paste all or part of these commands into the console before any of the profiles or profiles groups are referenced by other items in the configuration. This will leave the Outbound, Inbound, and Alert-Only profiles in the configuration.

This frees up space for nine other security profiles not part of IronSkillet.

```
delete profile-group Internal
delete profiles virus Internal-AV
delete profiles spyware Internal-AS
delete profiles vulnerability Internal-VP
delete profiles file-blocking Internal-FB
delete profiles wildfire-analysis Internal-WF
delete profiles virus Exception-AV
delete profiles spyware Exception-AS
delete profiles vulnerability Exception-VP
delete profiles url-filtering Exception-URL
```



---

## Common or per-device elements

---

Many of the configuration elements are common between Panorama and panos. The variance is the xpath branch naming where the elements sits in the config tree.

---

**Note:** The '\*' at the end of a template name denotes multiple files with the same leading text

---

### 12.1 Common snippets

These xml files are common across both platforms

- address
- device\_setting
- device\_system
- email\_scheduler\_simple
- external\_list
- profile\_group
- profiles\_\*
- report\_group\_simple
- tag
- zone\_protection\*

The rest are device specific based on xpath reference or configuration settings. Examples are deltas between rule configuration with pre/post in Panorama and log forwarding targets as Panorama or syslog.

## 12.2 Firewall specific

- log\_settings\_profiles
- reports\_simple
- rulebase\_\*
- shared\_log\_settings

## 12.3 Panorama specific

- device group
- log\_collector\_group
- log\_settings\_profiles
- panorama\*
- post\_rulebase\*
- pre\_rulebase\*
- reports\_simple
- shared\_log\_settings
- templates

### 13.1 8.1 Update Items

This includes changes from the 8.0 IronSkillet configurations

#### 13.1.1 Syntax changes

- `allow-http-range` in device settings

#### 13.1.2 8.1 new features

- WF file sizes
  - new file type script, set to max 2000 file size [available in later releases]

### 13.2 9.0 Update Items

This includes changes from the 8.1 IronSkillet configurations

#### 13.2.1 Syntax changes

- move packet cap xml element in spyware profile
- remove url 'block' stand-alone entry
- custom url categories
  - add 'type' value to allow config to commit
- sinkhole IPv4 address uses FQDN instead of IP value

## 13.2.2 9.0 new features

### Security profiles

- new url categories (risk, new domain)
  - set new categories to alert
  - over time move to custom dual category blocks (eg. parked + high)
- new pan cloud dns option in spyware profile
  - action = sinkhole with single packet capture
- AV profile and http2
  - set http2 decoder same as http for each profile

### Device settings

- API key lifetime
  - Initially set to a high value with configuration variable
  - Default in minutes -> 525,600 is 1 year

## 13.2.3 9.1 new features

### Security profiles

- new url categories (grayware, cryptocurrency)
  - set grayware to block
  - set cryptocurrency to alert

---

**Note:** these are shown with their initial 9.1 release but also supported in prior PAN-OS releases

---

---

## Release and Update History

---

Includes:

- template releases
- tools updates
- documentation revisions

### 14.1 9.1 Template Release History

Template content updates are high level. Details can be found in the template guides.

#### 14.1.1 0.0.1

Released January 22, 2020

- first release based on v9.0
- no release specific additions

### 14.2 9.0 Template Release History

Template content updates are high level. Details can be found in the template guides.

#### 14.2.1 0.0.4

Released January 22, 2020

- added grayware and cryptocurrency url categories
- added missing User tag log settings

- inclusion of validation skillets

### **14.2.2 0.0.3**

Released c September, 2019

- minor updates

### **14.2.3 0.0.2**

Released July 30, 2019

- Added password complexity and admin lockout elements
- Dynamic updates for GlobalProtect
- Opt-out default for the Palo Alto Networks EDL associated security rules
- Removed the IPv4 and IPv6 Bogon EDLs and associated security rules
- Updated the IPv4 sinkhole to use FQDN instead of an IP address
- Clean up for the baseline configuration to remove IPSEC, IKE, QoS defaults
- Clean up for URL Black-List and White-List category usage in profiles

### **14.2.4 0.0.1**

Released March 15, 2019

- migrated initial template from 8.1
- inclusion of new features per the 9.0 new features documentation

## **14.3 8.x Template Release History**

Template content updates are high level. Details can be found in the template guides.

### **14.3.1 1.0.6**

Released July 30, 2019

- Added password complexity and admin lockout elements
- Dynamic updates for GlobalProtect
- Opt-out default for the Palo Alto Networks EDL associated security rules
- Removed the IPv4 and IPv6 Bogon EDLs and associated security rules
- Updated the IPv4 sinkhole to use FQDN instead of an IP address
- Clean up for the baseline configuration to remove IPSEC, IKE, QoS defaults
- Clean up for URL Black-List and White-List category usage in profiles

### 14.3.2 1.0.5

Released March 18, 2019

Template Content

- added max lines for log csv output

### 14.3.3 1.0.4

Released January 8, 2019

Template Content

- updated virus profiles from 'default' to 'reset-both' so explicit blocking
- added set commands template as text file and Excel spreadsheet
- loadable default configurations include full xml and set commands
- update to the template stack snippet including <config> tree elements
- removed GTP logging elements since not supported on all hardware platforms

### 14.3.4 1.0.3

Released Oct 3, 2018

Template Content

- added a default security profile group based on the Outbound group

Documentation

- fixed errors in the tools installation instructions

### 14.3.5 1.0.2

Released August 30, 2018

Template Content

- modified device\_system type=dhcp configuration elements to fix dhcp-client commit error

### 14.3.6 1.0.1

Released: August 7, 2018

Template Content

- Device settings updates to increase security hardening
  - Prevent TCP and UDP buffer overflow and multi-part HTTP download evasions
  - Enable high DP load logging
  - Prevent App-ID buffer overflow evasion
  - set bypass-exceed-queue to 'no'
  - Prevent TCP and MPTCP evasions

- Include default login banner
- Correct url-filtering Alert-All profile to include command-and-control
- Set default interzone action to a drop instead of deny
- include firewall management interface options for dhcp-client, standard or cloud models
- include Panorama options for standard or cloud deployments
- using a tag attribute for the template version numbering

#### Documentation

- moved docs to readthedocs.io
- move to release-specific documentation

#### Template Archive

- moved to release branch per software release in github

### **14.3.7 1.0.0**

Released: May 10, 2018

- first release on github
- xml snippets and full config
- static pdf documentation

## **14.4 Tools Release Updates**

### **14.4.1 Jan 22, 2020**

- updated the build\_full\_config.py with the ability to merge snippets using same xpath

### **14.4.2 Jul 30, 2019**

- added build\_all.py to create all full configs and spreadsheets
- test\_set\_commands.py and test\_full\_config.py to load and test configuration changes

### **14.4.3 Jan 8, 2019**

- moved config variables from a python dictionary to a yaml format
- updated existing tools to support the yaml variables file
- added a utility to create the Excel spreadsheet from the set conf file
- removed the creation of default snippets output to loadable configs
- renamed the output from 'my configs' to 'loadable configs' for clarity

#### 14.4.4 Oct 3, 2018

- modified variable model to support python 3.5 instead of 3.6 and later

#### 14.4.5 August 7, 2018

- added the build\_full\_config utility to create a full template from the config snippets
- added the build\_my\_config utility
  - provide simple variable substitutions using the my\_variable inputs
  - store output into the my\_config folder with unique naming

#### 14.4.6 May 3, 2019

- fixed tools issue so will load the panw edl based security rules

### 14.5 Documentation Revisions

Documentation revisions outside of template-tooling updates. These are documented by date, not version.

#### 14.5.1 January 22, 2020

- addition of visual guide for panos
- validation skillet section added
- add 9.1 related content links

#### 14.5.2 July 30, 2019

- Move docs to their own doc branch and merge as a single doc set
- Add in associated template changes and new xml links (mgt user config and password complexity)
- Add a release variance doc to show deltas for new releases
- Addition of requirements and caveats to use IronSkillet
- Pointers to PanHandler and SkilletCLI as new tools to load configurations

#### 14.5.3 March 18, 2019

- added instructions to remove security profiles for reduced capacity VM-50
- updated with inclusion of max csv lines for log output

#### 14.5.4 Jan 8, 2019

- simplified repo main README for non-python users
- added documentation for the SET command spreadsheet
- added next-level directory README files for added context
- general edits for using tools based on tools changes
- added description for Panorama template variations in Panorama template docs

#### 14.5.5 Nov 2, 2018

- added instructions for editing the full configuration template variables in the GUI
- added instructions for editing the full configuration template variables using the console

#### 14.5.6 Oct 3, 2018

- fixed errors in the tools installation instructions

#### 14.5.7 August 7, 2018

- moved docs to readthedocs.io
- move to release-specific documentation

#### 14.5.8 May 10, 2018

- first release on github
- static pdf documentation