Release Notes for Forcepoint i-Series Appliances

Release Notes | i-Series Appliance | Updated: 07-Dec-2016

Applies to:	Forcepoint i-Series appliance v1.7, 1.7.1

Contents

The Forcepoint™ i-Series™ appliance is a component of Forcepoint TRITON AP-WEB with the Cloud Web Module. This web protection solution provides on-premises URL analysis and application/protocol detection for web traffic, along with centralized policy management and reporting capabilities in the cloud.

The i-Series appliance hosts the Forcepoint URL category master database, allowing the efficient analysis of web site request URLs. The appliance also provides protocol detection capabilities and policy enforcement.

When analysis indicates that a web request requires further examination, the appliance transparently routes that traffic to the cloud, where Forcepoint cloud service analytics are applied and policy is enforced. Management of on-premises appliances is also performed in the cloud.

You can deploy the Forcepoint i-Series appliance as a virtual appliance. For virtual appliance information, see the Getting Started Guide.

View detailed product user information in the following Help systems:

- Forcepoint i-Series Appliance Help
- Forcepoint Cloud TRITON Manager Help

Use these Release Notes to learn about important version 1.7 updates, as well as new product features, installation and upgrade tips, and resolved and known issues.

Important

- Beginning with version 1.5, appliance management access to the appliance bridge interfaces (B1 and B2) is always allowed. The option to block management access has been removed from the **Configuration > Networking** page. The functionality may be restored in a future version.
- NTLM2 Session authentication is not supported for Microsoft Active Directory. You should use either NTLMv1 or NTLMv2 authentication. See *Resolved and known issues* for workaround instructions.

Version 1.7 and 1.7.1 important updates

Release Notes | i-Series Appliance | Updated: 07-Dec-2016

Applies to:	Forcepoint i-Series appliance v1.7, 1.7.1

Version 1.7.1 of the Forcepoint i-Series appliance includes a critical fix that prevents a major system error.

Important

Because this issue was introduced in version 1.7.0, we strongly recommend that you upgrade appliances to version 1.7.1 as soon as possible, to avoid encountering this severe system error.

Post-upgrade known issue:

End-of-life notifications for version 1.7.1 may appear after the upgrade is completed, in a pop-up box and on the **Status > General** page. These notification are incorrect.

Workaround:

- Click OK to close the pop-up box.
- Ignore the message on the **Status > General** page. It will disappear in a few days. You can also restart the appliance to remove this message.

The version 1.7 release of the Forcepoint appliance addresses the following vulnerabilities:

- **Network Time Protocol (NTP) vulnerabilities**

  The NTP service was updated to resolve the following issues:

  CVE-2016-1547

CVE-2016-1548
CVE-2016-1549
CVE-2016-1550
CVE-2016-2516
CVE-2016-2517
CVE-2016-2518

- **OpenSSL vulnerabilities**
  OpenSSL libraries were updated to resolve the following issues:
  CVE-2016-2105
  CVE-2016-2106
  CVE-2016-2107
  CVE-2016-2108
  CVE-2016-2109
  CVE-2016-2176
- **Samba service vulnerability**
  Samba was updated to resolve the issue described in CVE-2016-2118.
- **Network Security Services (NSS) utilities vulnerability**
  NSS utilities were updated to resolve the issue described in CVE-2016-1950.

Version 1.7 product features

Release Notes | i-Series Appliance | Updated: 07-Dec-2016

Applies to:	Forcepoint i-Series appliance v1.7, 1.7.1

This section of the Release Notes describes the new features that are included in version 1.7 of the Forcepoint i-Series appliance:

- *Forcepoint rebranding*
- *Improved upgrade stability*
- *Improved system infrastructure*

See the Forcepoint TRITON AP-WEB (cloud) Release Notes for detailed information about all cloud portal changes.

Forcepoint rebranding

To support the transition from Raytheon | Websense to Forcepoint LLC, the appliance manager acquired a new look and feel in version 1.6.x. Forcepoint branding is extended in this release to the embedded Help system and the cloud portal certificate, as well as to external content, like the Knowledge Base.

Improved upgrade stability

The i-Series appliance is enhanced in this release to introduce greater stability for the upgrade process. Upgrade to version 1.7 includes an initial step to back up the appliance system by taking a “snapshot” of the current system and saving it for recovery purposes, if needed.

The version 1.7 snapshot will provide a rollback option for future upgrades, to ensure continuous appliance operations in the event that an upgrade is unsuccessful for some reason. Alerts provide the status of the backup operation.

New upgrade logs (for the last failed upgrade) can be uploaded by using the appliance command-line interface (CLI) **--upgrade-logs-only** directive of the **diags_upload** command. Example command syntax is:

```
diags_upload --upload-url http://www.upload_destination.com/
[--upload-username <username> --upgrade-logs-only]
```

Important

The infrastructure for the rollback feature is introduced in version 1.7.0, however, an unsuccessful upgrade to version 1.7.0 does not include the rollback function. The rollback function will be available if an upgrade to a future version of the appliance is unsuccessful.

Improved system infrastructure

This version of the appliance includes several enhancements and fixes for system infrastructure that result in improved stability and security.

- Network monitoring tools upgrades provide enhanced stability.
- Operating system upgrade contributes to improved security.
- Enhancements and fixes to the cloud proxy service provide greater stability and efficiency.
- Policy engine upgrade results in enhanced enforcement and security.
- Traffic analysis mechanism upgrade improves overall appliance stability and reliability.

Installation, deployment, and upgrade

Applies to:	Forcepoint i-Series appliance v1.7, 1.7.1

Installation

Installation and set up for the Forcepoint i-Series appliance are summarized on the Quick Start poster that was shipped with your appliance. Click here to view a copy of the quick start guide.

See the Getting Started Guide for information about system configuration.

Important
Use of Microsoft Internet Explorer 8 (or below) on a Windows XP machine is not supported.

If your network includes a firewall, you need to ensure that destination TCP ports are open for connection to the cloud service. By default, the appliance is configured to use standard destination ports 80 and 443 for these connections.

Note
Upgrade from a previous appliance version that uses different default port settings does not automatically change port configuration settings. If you want to use destination ports 80 and 443, you should modify appliance settings manually after the upgrade process.

Alternatively, and depending on your corporate firewall policy, you can configure your appliance to use the following ports, which are used for non-appliance connections to the cloud service:

Port	Purpose
8002	Configuration and policy update information retrieval from the Forcepoint cloud service. This port must be open for an i-Series appliance to retrieve periodic configuration setting and policy updates from the cloud service.
8081	Proxy service. This is where Forcepoint cloud-based content analysis is provided.

Port	Purpose
80	Notification page components. The default notification pages refer to style sheets and images served from the Forcepoint cloud service platform. For these pages to appear correctly, this web site is accessed directly (i.e., not through the Forcepoint cloud service).
443	Service administration. The Forcepoint administration portal is similarly unproxied. Otherwise, it would be possible for you to accidentally block access and then be unable to rectify the situation.

You can switch between the standard and alternative ports at any time using the appliance command-line interface (CLI). See the Getting Started Guide for detailed instructions about switching port settings.

You should also open the outbound Network Time Protocol (NTP) port (UDP 123) to allow time/clock synchronization in the system.

Note

The transfer of new password and appliance registration information between the cloud portal and the appliance takes several minutes. You may experience a delay when logging in after a change is made to these settings.

Deployment

Additional considerations should be examined for some i-Series appliance deployments, including those that use:

- an i-Series virtual appliance
- endpoint devices or PAC-enabled clients that communicate directly with the cloud

  See *Mixed-mode deployment issues* for information about handling traffic via these devices.

Virtual appliance

The i-Series virtual appliance may be deployed with or without the network bypass capability. Download the appliance image (OVF format) from the My Account

Downloads page, and see the Getting Started Guide for virtual appliance deployment instructions.

Note

If you want to deploy a virtual appliance with the network bypass capability, your hardware must support the ESXi DirectPath I/O function.

If you plan to deploy a virtual appliance, you should verify the following system requirements:

- VMware vSphere ESXi platform versions 5.1, 5.5, or 6.0
- 6 CPU cores, 12 GB RAM (minimum)
- 128 GB hard disk drive
- Optional: Silicom network bypass card (Silicom PE2G2BPI80-SD-R) with 2 dedicated network interfaces (must be installed on ESXi in VMDirectPath mode)

  Some models of HP hardware do not support VMDirectPath mode.

Mixed-mode deployment issues

If your network includes an i-Series appliance along with endpoint devices or PAC-enabled clients that communicate with the cloud directly (for example, roaming users), you may encounter additional deployment issues. You should consider the following port information before you deploy:

- Use of the site's egress as a policy connection is not supported. As a result, endpoint or PAC-enabled clients are treated as roaming users regardless of whether they are connected within the network LAN.
- Endpoint device and PAC-enabled client traffic directly to the cloud service in a network that includes an i-Series appliance is supported on ports 8081 and 8082. If the deployment requires the use of ports 80 and 443 for endpoint client traffic, please contact Forcepoint Technical Support.
- When a Forcepoint Endpoint requests a PAC file download, the cloud service can return a custom PAC file that first directs endpoint traffic to the appliance rather than redirecting it to the cloud service. Please contact Forcepoint Technical Support for assistance to activate this feature.
- Endpoint device traffic directly to the cloud service in a network that includes an i-Series appliance is supported on port 80, but traffic from a PAC-enabled client on port 80 is not supported.
- Applications that use HTTP (e.g., IM clients) may still try to use port 80 or 443 for outbound traffic. This traffic is intercepted and processed by the i-Series appliance, which may lead to inconsistent behavior. This potential problem should be checked on a per-site, per-application basis, and a resolution determined based on a customer's actual needs, for example:
  - Block the applications at the firewall level
  - Use other ports for the applications

Upgrade

Use the following steps to upgrade from a previous version of the Forcepoint i-Series appliance:

1. Click **Network Devices** in the cloud portal.
2. Select the appropriate appliance for the upgrade and click **Properties & Statistics**.
3. Click **Version History**.
4. Find the desired upgrade and click the **Download** icon in the Action column. This operation downloads the upgrade to the selected appliance.

   Clicking the **View** icon in the Description column opens the Release Notes for that upgrade.
5. In the i-Series appliance **Configuration > Upgrade Management** page, find the upgrade in the table at the top of the screen. The upgrade status should be **Downloaded** (you may need to refresh the screen to see the change). Click the **Install** icon to install the upgrade.

Important

Upgrade status may display as “Failed” after a successful upgrade. This incorrect error message may appear if you refresh the appliance user interface immediately after the upgrade operation.

Please wait approximately 5 minutes to refresh the user interface after the upgrade.

If the problem persists after this time period, please contact Forcepoint Technical Support.

Resolved and known issues

Release Notes | i-Series Appliance | Updated: 07-Dec-2016

Applies to:	Forcepoint i-Series appliance v1.7, 1.7.1

A list of resolved and known issues for the Forcepoint i-Series appliance is available in the Forcepoint Technical Library. If you are not already logged on to the My Account site, this link takes you to the log in screen.