Release Notes for Forcepoint I Series Appliances

Release Notes | I Series Appliance | Updated: 27-Jul-2018

The Forcepoint™ I Series™ appliance is a component of Forcepoint Web Security Cloud. 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 URL requests. 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 Deploying an I Series Appliance.

View detailed product user information in the following Help systems:

- Forcepoint I Series Appliance Help
- Forcepoint Web Security Cloud Help

Use these Release Notes to learn about important version 1.8, 1.8.1, and 1.8.2 updates; 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 1.8.2 important updates

Release Notes | I Series Appliance | Updated: 27-Jul-2018

The version 1.8.2 appliance release addresses the following vulnerabilities:

- **Linux kernel vulnerabilities**

  The CentOS kernel was updated to resolve the following issues:

  CVE-2017-5715

  CVE-2017-5753

  CVE-2017-5754
- Appliance-generated certificates now include the Subject Alternative Name field, which is required for Google Chrome version 58 and later.
- Appliance communications with the cloud service now use TLS 1.2.

Important

Download the **.iso** image file for a new version 1.8.2 installation on a physical appliance from the Forcepoint Downloads page.

New installation for the Forcepoint i500 virtual appliance (.ova file) for version 1.8.2 is not available.

Users on all platforms (virtual and physical) may upgrade to version 1.8.2 via the appliance manager **Configuration > Upgrade Management** page. See *Upgrade*, page 8, for more information.

Version 1.8.1 important updates

Release Notes | I Series Appliance | Updated: 27-Jul-2018

The Version 1.8.1 release of the Forcepoint I Series appliance addresses the following product issues:

- The I Series appliance did not correctly resolve external DNS servers during diagnostic testing.

  This issue has been resolved.

- An appliance sometimes incorrectly received a license expiration notice from the cloud service and could not recover.

  Product license behavior has been changed to allow a user with a valid license to perform a manual license update when this situation occurs.

  Log in as admin and run the following commands in the appliance command-line interface (CLI):

  ```
  cmd> device
  device> license
  license> update
  ```

Important

Download the **.iso** image file for a new version 1.8.1 installation on a physical appliance from the Forcepoint Downloads page.

New installation for the Forcepoint i500 virtual appliance (**.ova** file) for version 1.8.1 is not available.

Users on all platforms (virtual and physical) may upgrade to version 1.8.1 via the appliance manager **Configuration > Upgrade Management** page. See *Upgrade*, page 8, for more information.

Version 1.8 important updates

Release Notes | I Series Appliance | Updated: 27-Jul-2018

The version 1.8 appliance release addresses the following vulnerabilities:

- **OpenSSL vulnerabilities**

  OpenSSL libraries were updated to resolve the following issues:

  CVE-2016-2177

  CVE-2016-2178

  CVE-2016-2179

  CVE-2016-2180

  CVE-2016-2181

  CVE-2016-2182

CVE-2016-6302

CVE-2016-6304

CVE-2016-6306

- **Samba service vulnerability**

  Samba was updated to resolve the issue described in CVE-2016-2119.

- **Linux kernel vulnerability**

  NSS utilities were updated to resolve the issue described in CVE-2016-5195.

Version 1.8 product features

Release Notes | I Series Appliance | Updated: 27-Jul-2018

This section of the Release Notes describes the new features that are included in version 1.8 of the Forcepoint I Series appliance:

- *Improved upgrade stability*
- *Appliance manager user interface improvements*

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

Improved upgrade stability

The I Series appliance upgrade to version 1.7 included 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 provides a rollback option for the upgrade to version 1.8 and later, 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]
```

Note

The rollback function may fail on older model I Series appliances due to a BIOS formatting issue. In this situation, the appliance must be re-imaged.

Several fixes and enhancements for the upgrade process are included in this release, providing a more secure and reliable appliance upgrade.

Appliance manager user interface improvements

- The appliance manager **Status > General** page displays a clear indicator of connectivity status with the Forcepoint cloud service and for the most recent configuration and policy updates from the cloud service.

  The Forcepoint Cloud Service Updates section displays connectivity as either **Connected** or **Disconnected**. The **Last policy update** field contains the date/time of the most recent configuration and policy settings download from the cloud service.
- The Platform field on the **Configuration > System Information** page displays the appliance platform as either **i500** or **i500v** (for the virtual appliance).
- The upgrade history table Status column entry defines the action that occurred on the specified date/time (**Configuration > Upgrade Management**).

Installation, deployment, and upgrade

Release Notes | I Series Appliance | Updated: 27-Jul-2018

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.
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).

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 Forcepoint My Account Downloads page.

> **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: 27-Jul-2018

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