F5® Herculon™ SSL Orchestrator™: Setup

Version 13.1-3.0

Table of Contents

What is F5 Herculon SSL Orchestrator? 5
What is F5 Herculon SSL Orchestrator? 5

Terminology for Herculon SSL Orchestrator 7
Terminology for Herculon SSL Orchestrator 7

Configuring the System for F5 Herculon SSL Orchestrator 9
Overview: Configuring the system for F5 Herculon SSL Orchestrator 9
Using the Herculon SSL Orchestrator setup wizard 9
Backing up your BIG-IP configuration 11
Modifying your Herculon SSL Orchestrator configuration 11
Undeploying your Herculon SSL Orchestrator configuration 11
Diagnosing your Herculon SSL Orchestrator deployment 12

Setting Up a Basic Configuration 13
Overview: Setting up a basic configuration 13
Configuring general properties 13
Configuring logging 15
Configuring an ingress and egress device on one system 16
Configuring an ingress device (for separate ingress and egress devices) 18
Configuring an egress device (for separate ingress and egress devices) 20
Configuring the system for transparent proxy 23
Configuring the system for explicit proxy 23
Configuring the system for both transparent and explicit proxies 24

Creating Services, Service Chains, and Classifier Rules 27
Overview: Creating services, service chains, and classifier rules 27
Creating inline services for service chains 27
Creating ICAP services 29
Creating receive-only services for traffic inspection 30
Creating service chains to link services 30
Creating TCP service chain classifier rules 31
Creating UDP service chain classifier rules 33

Importing and Exporting Configurations for Deployment 35
Overview: Importing and exporting configurations for deployment 35
Importing new configurations for deployment 35
Importing past configurations for deployment 36
Exporting configurations for deployment 36

Setting up Herculon SSL Orchestrator in a High Availability Environment 39
Overview: Setting up Herculon SSL Orchestrator in a high availability environment 39
Task summary for deploying in a high availability environment 40
Installing an updated RPM file 41
Configuring the network for high availability 41
Synchronizing the device group 43

Setting up a basic configuration for deployment....44
Task summary for diagnosing and fixing high availability deployment.... 44
Verifying deployment and viewing logs....44
Verifying the RPM file version on both devices.... 45
Configuring general properties and redeploying.... 45
Reviewing error logs and performing recovery steps.... 45

Using Herculon SSL Orchestrator Analytics....47
Overview: About Herculon SSL Orchestrator analytics....47
About analytics dashboard capabilities....47
Timeline capabilities....48
Customizing timeline capabilities.... 48
Chart capabilities.... 48
Customizing chart capabilities.... 49
Table capabilities....49
Customizing table capabilities....49
Charting bytes in, bytes out, and hit count over time.... 50
Comparing statistics on the top virtual servers.... 50
Viewing the top sites bypassed....51
Viewing the top sites decrypted.... 51
Viewing the most used client ciphers and protocols.... 52
Finding where the top server ciphers and protocols are used.... 52
Scheduling reports to be sent.... 52

Legal Notices.... 55
Legal notices....55

What is F5 Herculon SSL Orchestrator?

What is F5 Herculon SSL Orchestrator?

F5® Herculon™ SSL Orchestrator™ provides an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize the efficient use of that existing security investment. This solution centralizes and consolidates SSL inspection across complex security architectures, allowing you flexible deployment options to decrypt and re-encrypt user traffic across the Internet and web-based applications. It supports policy-based management and steering of traffic flows to third-party security devices such as firewalls, intrusion prevention systems (IPS), anti-malware, data loss prevention (DLP), and forensics tools. It provides a wide range of SSL orchestration analytics that you can easily customize across multiple dimensions based on specified ranges of time.

The Herculon SSL Orchestrator single platform for unified inspection allows for the greatest flexibly without architectural changes to prevent new blind spots from emerging.

Some of the key functions include:

- Dynamic security service chaining that leverages context-based policies to efficiently deploy security, reduce administrative overhead, and effectively utilize security resources
- Centralized management of the SSL decrypt and re-encrypt function
- Inspection of all traffic for malware and data exfiltration with a multi-layered approach
- Flexible deployment modes to easily integrate the latest encryption technologies across your entire security infrastructure
- High availability with best-in-class load-balancing, health monitoring, and SSL offload capabilities

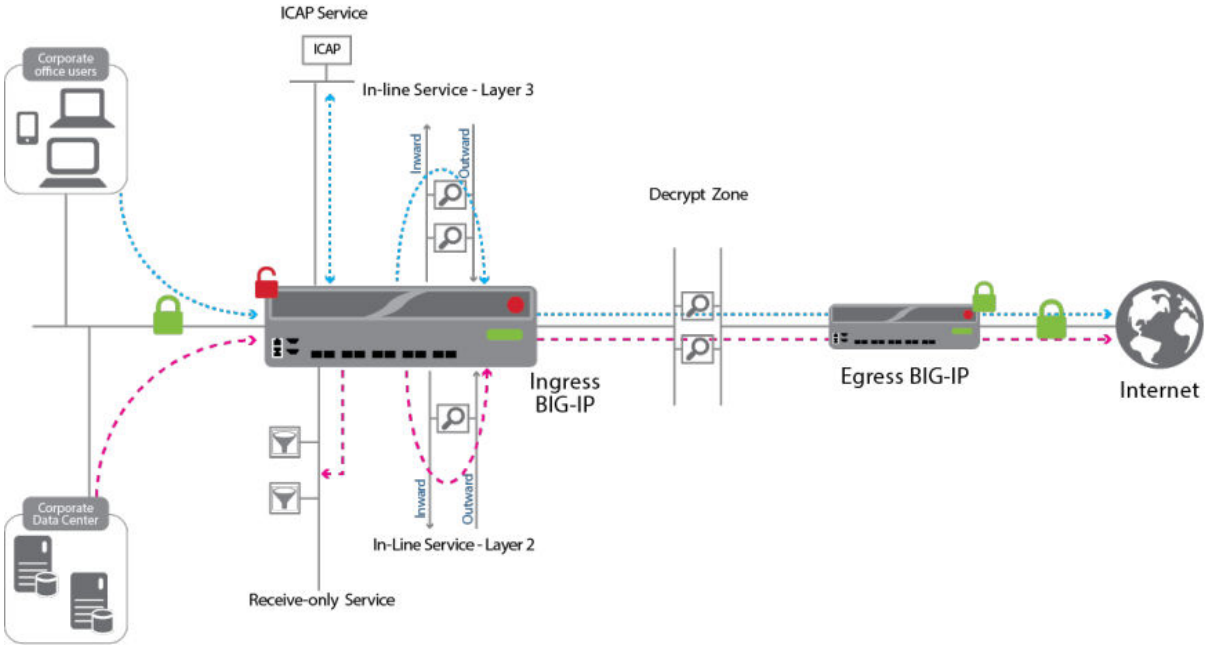

Figure 1: Herculon SSL Orchestrator solution

Terminology for Herculon SSL Orchestrator

Terminology for Herculon SSL Orchestrator

This section defines some of the terms used in this document.

- **Certificate Authority (CA) certificate**

  This implementation requires a Certificate Authority PKI (public key infrastructure) certificate and matching private key for SSL Forward Proxy. Your TLS clients must trust this CA certificate to sign server certificates.
- **Decrypt zone**

  A decrypt zone refers to the network region between separate ingress and egress BIG-IP® devices where cleartex data is available for inspection. Basically an extra inline service can be placed at the end of every service chain for additional inspection. You cannot configure a decrypt zone in the scenario where a single BIG-IP system handles both ingress and egress traffic because the decrypt zone does not exist.
- **Egress device**

  The egress BIG-IP system is the device (or Sync-Failover device group) that receives the traffic after a connection traverses the chosen service chain and then routes it to its final destination. In the scenario where both ingress and egress traffic are handled by the same BIG-IP system, egress refers to the VLAN(s) where traffic leaves the BIG-IP system to the Internet.
- **ICAP services**

  Each ICAP service uses the ICAP protocol (https://tools.ietf.org/html/rfc3507) to refer HTTP traffic to one or more Content Adaptation device(s) for inspection and possible modification. You can add an ICAP service to any TCP service chain, but only HTTP traffic is sent to it, as we do not support ICAP for other protocols. You can configure up to ten ICAP services using F5® Herculon™ SSL Orchestrator™. For more information on ICAP services, refer to the *Creating ICAP services* section.
- **Ingress device**

  The ingress BIG-IP system is the device (or Sync-Failover device group) to which each client sends traffic. In the scenario where both ingress and egress traffic are handled by the same BIG-IP system, ingress refers to the VLAN(s) where the client sends traffic. The ingress BIG-IP system (or ingress VLAN(s)) decrypts the traffic and then based on protocol, source, destination, and so on, classifies it and passes each connection for inspection based on service chains you will configure (or allows certain connections to bypass service-chain processing based on your selections).
- **Inline services**

  Inline services pass traffic through one or more service (inspection) devices at Layer2 (MAC)/Bump-in-the-wire or Layer3 (IP). Each service device communicates with the ingress BIG-IP device over two VLANs called *Inward* and *Outward*which carry traffic toward the intranet and the Internet respectively. You can configure up to ten inline services, each with multiple defined devices, using Herculon SSL Orchestrator.
- **Receive-only services**

  Receive-only services refer to services that only receive traffic for inspection, and do not send it back to the BIG-IP system. Each receive-only service provides a packet-by-packet copy of the traffic (e.g. plaintext) passing through it to an inspection device. You can configure up to ten receive-only services using Herculon SSL Orchestrator. For more information on receive-only services, refer to the *Creating receive-only services for traffic inspection* section.
- **Service chain classifier rules**

Each service chain classifier rule chooses ingress connections to be processed by a service chain you configure (different classifier rules may send connections to the same chain). Each classifier rule has four filters.The filters match source (client) IP address, destination (which can be IP address, IP Intelligence category, IP geolocation, domain name, domain URL Filtering category, or server port), and application protocol (based on port or protocol detection). Filters can overlap so the implementation chooses the classifier rule with the most specifc matches for each connection.

For more information on service chain classifier rules, refer to the *Creating TCP service chain classifier rules* section and/or the *Creating UDP service chain classifier rules* section.

- **Service chains**

  Herculon SSL Orchestrator service chains process specific connections based on classifier rules which look at protocol, source and destination addresses, and so on. These service chains can include four types of services (Layer 2 inline services, Layer 3 inline services, receive-only services, and ICAP services) you define, as well as any decrypt zone between separate ingress and egress devices). For more information on service chains, refer to the *Creating service chains to link services* section.

- **SNAT**

  A SNAT (Secure Network Address Translation) is a feature that defines routable alias IP addresses that the BIG-IP system substitutes for client IP source addresses when making connections to hosts on the external network. A **SNAT pool** is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool should not be self IP addresses.

- **Sync-Failover device group**

  A Sync-Failover device group (part of the Device Service Clustering (DSC®) functionality) contains BIG-IP devices that synchronize their configuration data and failover to one another when a device becomes unavailable. In this configuration, a Sync-Failover device group supports a maximum of two devices.

- **Transparent/Explicit Proxy**

  You can operate in transparent and/or explicit proxy mode. A transparent proxy intercepts normal communication without requiring any special client configuration; clients are unaware of the proxy in the network. In this implementation, the transparent proxy scheme can intercept all types of TLS and TCP traffic. It can also process UDP and forward other types of IP traffic. The explicit proxy scheme supports only HTTP(S) per RFC2616. In addition, transparent proxy supports direct routing for policy-based routing (PBR) and Web Cache Communication Protocol (WCCP) that are dependent on networking services to support both protocols, while explicit proxy supports manual browser settings for proxy auto-config (PAC) and Web Proxy Autodiscovery Protocol (WPAD) that require additional iRule configurations (not included) to provide the PAC/WPAD script content.

Configuring the System for F5 Herculon SSL Orchestrator

Overview: Configuring the system for F5 Herculon SSL Orchestrator

To set up your system for decrypting and encrypting outbound SSL/TLS traffic, you need to use the F5® Herculon™ SSL Orchestrator™ Setup Wizard which initially guides you through basic minimal setup configuration. When you have completed the basic setup using the Setup Wizard, the Herculon SSL Orchestrator configuration utility assists you with the rest of your configuration.

Note: *If you are implementing a high availability environment for Herculon SSL Orchestrator, review the Setting up Herculon SSL Orchestrator in a High Availability Environment section for more detailed information.*

Using the Herculon SSL Orchestrator setup wizard

Before you start this task:

Make sure you set up a management IP address, netmask, and default routing on your system.

Note: *If at any time during your configuration you need to return to the F5® Herculon™ SSL Orchestrator™ Setup Wizard, simply click the F5 logo in the upper-left corner of the configuration utility, and on the Welcome screen, click the* ***Run the Setup Utility*** *link.*

The Herculon SSL Orchestrator Setup Wizard guides you through the basic, minimal setup configuration for Herculon SSL Orchestrator.

1. On the Welcome screen, click **Next**.
2. On the License screen, click **Activate**.
3. On the EULA screen, click **Accept**.
   The license activates and the system reboots for the configuration changes to take effect.
4. After the system reboots, click **Continue**.
5. On the Device Certificates screen, click **Next**.
6. On the Platform screen, for the **Management Port Configuration** setting, click **Manual**.

   The **Management Port** setting should include the management interface details that were previously created.
7. In the **Host Name** field, type the name of this system.

   The Host Name must be a fully qualified domain name.

   For example, `www.siterequest.com`.
8. In the User Administration area, type and confirm the Root Account and Admin Account passwords, and click **Next**.

   The Root Account provides access to the command line, while the Admin Account accesses the user interface.

   The system notifies you to log out and then log back in with your username and new password.
9. Click **OK**.
   The system reboots.
10. (Optional) On the Network Time Protocol (NTP) screen, in the **Address** field, type the IP address of the NTP server to synchronize the system clock with an NTP server, and click **Add**.

11. Click **Next**.
    The Domain Name Server (DNS) screen opens.
12. (Optional) To resolve host names on the system, set up the DNS and associated servers:
    a) For the **DNS Lookup Server List**, in the **Address** field, type the IP address of the DNS server and click **Add**.
    b) If you use BIND servers, add them in the **BIND Forwarder Server List**.
    c) For local domain lookups to resolve local host names, add them in the **DNS Search Domain List**.
    d) Click **Next**.

    The Internal VLAN screen opens.

    Note: *If you plan to later use the DNSSEC option in the configuration utility, you must set up DNS using the Herculon SSL Orchestrator Setup Wizard. Otherwise, this step is optional.*

    ---

13. Specify the **Self IP** settings for the internal network:
    a) In the **Address** field, type a self IP address.
    b) In the **Netmask** field, type a network mask for the self IP address.
    c) For the **Port Lockdown** setting, retain the default value.
14. For the **VLAN Tag ID** setting, retain the recommended default value, **auto**.
15. For the **Interfaces** setting:
    a) From the **VLAN Interfaces** list, select an interface number.
    b) From the **Tagging** list, select **Tagged** or **Untagged**.
       Select **Tagged** when you want traffic for that interface to be tagged with a VLAN ID.
    c) Click **Add**.
16. Click **Next**.
    This completes the configuration of the internal self IP addresses and VLAN, and the External VLAN screen opens.
17. Specify the **Self IP** setting for the external network:
    a) In the **Address** field, type a self IP address.
    b) In the **Netmask** field, type a network mask for the self IP address.
    c) For the **Port Lockdown** setting, retain the default value.
18. In the **Default Gateway** field, type the IP address that you want to use as the default gateway to the external VLAN.
19. For the **VLAN Tag ID** setting, retain the recommended default value, **auto**.
20. Click **Next**.
    This completes the configuration of the external self IP addresses and VLAN.
21. On the Forward Proxy Certificate screen, do the following:
    a) In the **Certificate Name** field, select **Create New** and type a certificate name.
    b) In the **Certificate Source** field, select either **Upload File** and click **Choose File**, or select **Paste Text** and copy and paste your certificate source.
    c) In the **Key Source** field, select either **Upload File** and click **Choose File**, or select **Paste Text** and copy and paste your key source.
    d) From the **Security Type** list, select either **Normal** or **Password**.
22. Click **Next**.
23. On the Logging screen, under **Publisher Type**, select either **local** or **splunk**.
    - If you select **local** as your **Publisher Type**, specify the **Destination** as either **local-db** or **local-syslog** and click **Next**.

Note: *This determines the destination of your logs as being either a local database or a local syslog server.*

- If you select **splunk** as your **Publisher Type**:

a) For **Protocol**, select either **TCP** or **UDP**.
b) Type the **IP** address and the **Port** of the splunk server.
c) Click **Next**.

You are now ready to proceed to the second part of the configuration where you follow additional instructions to finalize your system for Herculon SSL Orchestrator.

Backing up your BIG-IP configuration

Before beginning the Herculon SSL Orchestrator configuration, or before you make substantial changes, we strongly recommend you back up the BIG-IP configuration using the following steps. This allows you to restore the previous configuration in case of any issues.

1. On your system, click **System** > **Archives**.
2. To initiate the process of creating a new UCS archive (back up), click **Create**.
3. In the **File Name** box, type a name for the file. This name must be a unique name.
4. Click **Finished**.
5. To restore the configuration from a UCS archive, go to **System** > **Archives.**
6. Select the name of the UCS file you want to restore and click **Restore**.

Your BIG-IP configuration is now safely restored.

Modifying your Herculon SSL Orchestrator configuration

We recommend that you back up your BIG-IP® configuration prior to making any changes to your F5® Herculon™ SSL Orchestrator™ configuration. Refer to the *Backing up the BIG-IP Configuration* section of this document for more information.

You can modify your existing Herculon SSL Orchestrator configuration if you need to make changes.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. Modify your configuration and then click **Deploy**.

See the *Diagnosing your Herculon SSL Orchestrator deployment* section for more detailed information on how to monitor the success or failure of your configuration modification. If successful, your existing configuration is now updated.

Undeploying your Herculon SSL Orchestrator configuration

We recommend that you back up your BIG-IP® configuration prior to making any modifications to your F5® Herculon™ SSL Orchestrator™ configuration. Refer to the *Backing up the BIG-IP configuration* section of this document for more information.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. Click **Undeploy**.

See the *Diagnosing your Herculon SSL Orchestrator deployment* section for more detailed information on how to monitor the success or failure of your device undeployment. If successful, your entire configuration is now removed from your system.

Diagnosing your Herculon SSL Orchestrator deployment

You can diagnostically monitor each deployment and undeployment for a device configuration whether you are deploying a single device or multiple boxes in a high availability (HA) device group. The system displays an application status message above the network diagram indicating whether your device or device group has successfully `Deployed` or suffered an `Error`.

When there are multiple devices in a device group in an HA scenario, the application status message displays the state of the deployment as one system. For example, if two out of four devices in a device group deploy with errors, the application status message displays `2 Error`, indicating two devices suffered an error during deployment.

If you click **View Details** next to the application status message when you have multiple devices in a sync group, the Application Status dialog box opens. The Application Status table lists each BIG-IP® device with individual links to the Diagnostic screen. The Diagnostic screen displays the current device's deployment information and assists in further diagnosing any issues.

After completing a F5® Herculon™ SSL Orchestrator™ configuration deployment, or if you are performing an undeployment, you can diagnose your deployment status.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. On the General Properties screen, click either **Deploy** or **Undeploy**.

   Above the network diagram, the application status displays a spinning wheel with the message `Currently being deployed` or `Currently being undeployed`.

   Once the process is complete, the application status message displays `Deployed`, `Undeployed`, or `Error`.
3. If you have multiple devices in a device group, click **View Details**. If you are deploying or undeploying a single device, proceed to step 4.

   If your deployment or undeployment is successful, the Diagnostic screen opens.

   If your deployment or undeployment is not successful, the Application Status dialog popup opens showing each BIG-IP device with individual links to the Diagnostic screen.
4. Click **OK** to close the Application Status dialog popup table, or click the link in the Details column for a particular device to open the Diagnostic screen.
   The Application Diagnostic area shows details for the current device that you selected. This is information you can use to further diagnose your application status.
5. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Diagnostic** to view diagnostic information on your current device.

The Diagnostic screen opens.

Setting Up a Basic Configuration

Overview: Setting up a basic configuration

This section contains general information that the system needs before you can configure services and service chains. The F5® Herculon™ SSL Orchestrator™ configuration utility will assist you with configuring logging settings, setting up ingress and egress devices as one system or separate systems, and configuring the system for transparent proxy and explicit proxy.

Configuring general properties

You must provide general information that the system needs so that you can then set up ingress and egress devices, create services and service chains, and create classifier rules using the Herculon SSL Orchestrator configuration utility.

Note: *By default, during the Herculon SSL Orchestrator deployment process, the system database value for Traffic Management Microkernel (TMM) fast forward is automatically disabled (set to "false"). To ensure your Herculon SSL Orchestrator deployment works properly, make sure the system database value for TMM fast forward remains disabled throughout the deployment. If you are not using Herculon SSL Orchestrator and need the system database value for TMM fast forward enabled, it must be manually changed.*

---

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. For the **Application Service Name** field, `ssloApp` is the default name for this configuration.
3. From the **Do you want to setup separate ingress and egress devices with a cleartext zone between them?** list, select one of the options:
   - If the same BIG-IP system receives both ingress and egress traffic on different networks, use **No, use one BIG-IP device for ingress and egress**.
   - If you are configuring separate devices for ingress and egress traffic, use **Yes, configure separate ingress and egress BIG-IP devices**.
4. From the **Which IP address families do you want to support?** list, select whether you want this configuration to **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**.
   If you do not choose to support both address families, you must configure IP addresses in the family you select for all IP address fields in this application. If you choose **Both IPv4 and IPv6**, you can send intercepted IPv6 traffic through an IPv4 Layer 3 service device.
5. From the **Which proxy schemes do you want to implement?** list, select whether the system operates in transparent proxy mode, explicit proxy mode, or both.
   - Use **Implement transparent proxy only** for the system to operate in transparent proxy mode. The transparent proxy scheme can intercept all types of TLS and TCP traffic. It also processes UDP traffic and forwards all other types of traffic. The transparent proxy requires no client configuration modifications.
   - Use **Implement both transparent and explicit proxies** for the system to operate in explicit and transparent proxy modes simultaneously.
   - Use **Implement explicit proxy only** for the system to operate in explicit proxy mode. The explicit proxy scheme supports only HTTP(S) per RFC2616. If you choose to configure an explicit proxy, assign a specific IP address and TCP port where the HTTP explicit-proxy clients connect.

Note: *When configuring a single device Herculon SSL Orchestrator transparent proxy in front of an explicit proxy, Herculon SSL Orchestrator can transparently intercept SSL traffic tunneled through an explicit proxy and selectively forward the decrypted user traffic through the security service chain for proper inspections. Afterwards, the user traffic is sent back to the BIG-IP, which re-encrypts the traffic and sends to the explicit proxy. User traffic of certain categories may also be rejected by the BIG-IP or bypass the security inspections.*

Note: *When transparently decrypting traffic to upstream explicit proxies in a two device Herculon SSL Orchestrator deployment, the SSL forward proxy interception only occurs on the ingress device (decryption, service chaining, and re-encryption occur on the ingress device, while the encrypted plaintext traffic will pass through the egress device). In addition, all classifier rules apply to traffic inside HTTP CONNECT tunnels except for rules bypassing SSL during the TLS handshake phase. Rules bypassing SSL during the TLS handshake phase do not apply because SSL forward proxy cannot reuse the same HTTP CONNECT tunnel to the explicit proxy for the bypassed flow.*

6. From the **Do you want to pass UDP traffic through the transparent proxy unexamined?** list, select one of the options:
   - Use **Yes, pass all UDP traffic unexamined** to pass UDP traffic through without inspecting it.
   - Use **No, manage UDP traffic by classification** to configure specific service chain classifier rules for UDP traffic.

   This option is available only if you select **Implement transparent proxy only**.
7. From the **Do you want to pass non-TCP, non-UDP traffic through the transparent proxy?** list, select one of the options:
   - Use **Yes, pass non-TCP, non-UDP traffic** (such as IPsec, SCTP, OSPF, and so on) if you want the system to pass all traffic that is not TCP or UDP through the transparent proxy. If you choose this option, this traffic will not be classified or processed by any service chain.
   - Use **No, block all non-TCP, non-UDP traffic** (such as IPsec, SCTP, OSPF, and so on.) for the system to block all non-TCP and non-UDP traffic.

   This option is available only if you select **Implement transparent proxy only**.
8. From the **Which is the SSL Forward Proxy CA certificate?** list, select the Certificate Authority (CA) certificate that your clients will trust to authenticate intercepted TLS connections.
9. From the **Which is the SSL Forward Proxy CA private key?** list, select the corresponding private key.

   You import the CA certificate and private key while configuring the Setup Wizard. If you did not use the Setup Wizard, you must import a CA certificate before you can use this functionality.
10. In the **What is the private-key passphrase (if any)?** field, type the private-key passphrase.

    If the key does not have a passphrase, leave the field empty.
11. From the **Which CA bundle is used to validate remote server certificates?** list, select the CA bundle that validates the remote server certificates.

    The CA bundle is the collection of root and intermediate certificates for the CA you trust to authenticate servers where your clients might connect. The CA bundle is also known as the local trust store.
12. From the **Should connections to servers with expired certificates be allowed?** list, select one of the two options to determine what happens with connections to servers with expired certificates:
    - Use **Yes, allow connections to servers with expired certificates** to allow connections to the servers that have expired certificates.
    - Use **No, forbid connections to servers with expired certificates** to prevent connections to servers that have expired certificates.

Remote servers can present expired certificates. Allowing connections to servers with expired certificates can cause a security risk.

13. From the **Should connections to servers with untrusted certificates be allowed?** list, select one of the two options to determine what happens with connections to servers with untrusted certificates:
    - Use **Yes, allow connections to servers with untrusted certificates** to allow connections to the servers that have untrusted certificates.
    - Use **No, forbid connections to servers with untrusted certificates** to prevent connections to servers that have untrusted certificates.

    Remote servers can present untrusted certificates. Allowing connections to servers with untrusted certificates can cause a security risk.
14. If strict updates should protect the configuration, select the check box for **Should strict updates be enforced for this application?**.

    If you select this option, you cannot manually modify any settings produced by the application. Once you disable this option, you can manually change your configuration. You should enable this setting to avoid misconfigurations that can cause an unusable application.

    F5 recommends you enable this setting to avoid misconfigurations that could result in an unusable application and F5's ability to support your product.
15. Click **Save**.

You have provided the basic configuration the system requires for Herculon SSL Orchestrator.

You can now set up ingress and egress devices, configure transparent or explicit proxies for the system, and create services, service chains, and classifier rules.

Configuring logging

Before configuring logging for F5® Herculon™ SSL Orchestrator™, complete all areas in General Properties. Refer to the *Configuring general properties* section of this document for more information.

You can generate log messages to help you monitor (and optionally debug) system activity. And you can choose the level of logging you want the system to perform. Log messages may be sent to one or more external log servers (preferred) and/or stored on the BIG-IP® device (less desirable because BIG-IP devices have limited log storage capacity).

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. Scroll down to the Logging Confguration area to the **What SSL Intercept logging level do you want to enable?** list, and select the level of logging you want the system to perform.
    - Use **Errors. Log only functional errors** to log errors related to how Herculon SSL Orchestrator functions.
    - Use **Normal. Log connection data as well as errors** to log per-connection data in addition to functional errors.
    - Use **Debug. Log debug data as well as normal level data** to log debug data as well as connection data and functional errors. Because this logging level consumes more resources on the BIG-IP system, use this mode only during setup or troubleshooting.
3. From the **Which Log Publisher will process the log messages?** list, select whether an existing log publisher object processes the log messages or does not process the log messages and sends the messages to syslog-ng.
    - Use **None (Send log messages to syslog-ng)** to send log messages to the system management plane syslog-ng subsystem. This option is not recommended for use in production systems.

- Otherwise, from the list, select the Log Publisher you created. A Log Publisher delivers log messages to one or more Log Destinations. Log Destinations may include Syslog, ArcSight, Splunk, and other log servers.

We strongly recommend that you use a Log Publisher for good system performance. The `syslog-ng` service is useful for Errors-only logging but is too slow for Normal or Debug logging when the system is used in production. A Log Publisher delivers log messages to one or more Log Destinations. Log Destinations may include Syslog, ArcSight, Splunk, and other log servers as well as the BIG-IP system's local log database. To use a Log Publisher, it must already be present on the system.

4. From the **What kind of statistics do you want to record?** list, select the type of statistic the system records. This implementation can collect usage data for connections, service chains, services, and so on. The implementation can also record remote domain names and TLS cipher suites for TLS connections if you wish, but gathering such data consumes more system resources.

   Domain names are taken from remote server PKI certificates (or client SNI in the case of Dynamic Domain Bypass) and may include a wild card. TLS cipher suites may not be recorded when a connection bypasses interception.

   If you choose to collect any statistics, the BIG-IP system starts saving extra data in memory for the use of integration with performance reporting systems like Splunk or BIG-IP iStats integration.

   - Use **None** if you do not want the system to record statistics.
   - Use **Usage counters only (No remote-domain+cipher records)** to record usage counters only and not statistics on remote-domain and cipher records.
   - Use **Usage counters and remote-domain+cipher records (may slow system)** to record both usage counters and remote-domain and cipher records. This option can slow performance on your system.
5. Click **Save**.

You have configured logging options and completed the basic Herculon SSL Orchestrator configuration.

Configuring an ingress and egress device on one system

The ingress device is either a device or a Sync-Failover device group where each client sends traffic. The egress device is either a device or a Sync-Failover device group that receives traffic after a connection travels through the specified service chain and directs the traffic to the final destination.

If both the ingress and egress traffic are used by the same BIG-IP® system, the ingress device is one or more ingress VLANs where the clients send traffic. The ingress device decrypts the traffic and then, based on protocol, source, and destination, classifies the traffic and passes each connection for inspection.

If both the ingress and egress traffic are used by the same BIG-IP system, the egress device is one or more egress VLANs where the clients receive traffic.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. If you have only one BIG-IP system, from the **Do you want to setup separate ingress and egress devices with a cleartext zone between them?** list, select **No, use one BIG-IP device for ingress and egress**.
3. From the **Which IP address families do you want to support?** list, select whether you want this configuration to **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**.
   If you do not choose to support both address families, you must configure IP addresses in the family you select for all IP address fields in this application. If you choose **Both IPv4 and IPv6**, you can send intercepted IPv6 traffic through an IPv4 Layer 3 service device.
4. From the **Which is the SSL Forward Proxy CA certificate?** list, select the Certificate Authority (CA) certificate that your clients will trust to authenticate intercepted TLS connections.

5. From the **Which is the SSL Forward Proxy CA private key?** list, select the corresponding private key.

   You import the CA certificate and private key while configuring the Setup Wizard. If you did not use the Setup Wizard, you must import a CA certificate before you can use this functionality.
6. In the **What is the private-key passphrase (if any)?** field, type the private-key passphrase.

   If the key does not have a passphrase, leave the field empty.
7. From the Ingress Device Configuration area, for the **Which VLAN(s) will bring client traffic to the transparent proxy?** setting, select one or more VLANs where transparent-proxy ingress traffic will arrive.
8. From the **How should a server TLS handshake failure be handled?** list, select whether you want the connection to fail or bypass the connection.
9. From the **DNS query resolution** list, select whether to permit the system to send DNS queries directly out to the Internet, or specify one or more local forwarding nameservers to process all DNS queries from Herculon SSL Orchestrator.
   - If you select **Send DNS queries directly to nameservers across the internet**, proceed to step 10.
   - If you select **Send DNS queries to forwarding nameservers on the local network**, proceed to step 11.
10. From the **Do you want to configure local/private DNS zones?** list, select whether you do, or do not, want to configure local or private DNS zones.
    - If you select **No, do not configure any local/private DNS zones**, proceed to step 13.
    - If you select **Yes, configure local/private DNS zones**, proceed to step 12.
11. In the **Which local forwarding nameserver(s) will resolve DNS queries from this solution?** field, type the IP address of local nameservers that will resolve all DNS queries from this implementation and click **Add**. Once you have added the necessary nameserver IP addresses, proceed to step 13.
12. In the **List local/private Forward Zones** setting, click **Add** and type the IP address of one or more nameservers.
13. From the **Do you want to use DNSSEC to validate DNS information?** list, select whether you do, or do not, want to use DNSSEC to validate the DNS information.
14. In the Egress Device Configuration area, from the **Do you want to SNAT client IP addresses?** list, select whether you do, or do not, want to define SNAT addresses.
    - If you select **No, pass client addresses unaltered**, proceed to step 17.
    - If you select **Yes, SNAT (replace) client addresses**, proceed to step 15.
15. From the **Do you want to use a SNAT Pool?** list, select whether you want to use a SNAT pool or SNAT auto map to translate addresses.
    - If you select **Yes, define SNAT Pool addresses for good performance**, proceed to step 16.
    - If you select **No, use SNAT Auto Map (not recommended)**, proceed to step 17.
16. Options to provide SNAT addresses will vary, whether you selected **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**. Enter at least as many IP host addresses as the number of TMM instances on the ingress device. Type address must be uniquely assigned and routed to the ingress device. It is best to assign addresses which are adjacent and grouped under a CIDR mask, for example, 203.0.113.8 up through 203.0.113.15 which fill 203.0.113.8/29.
    - In the **IPv4 SNAT addresses** field, type the IPv4 SNAT address.
    - In the **IPv6 SNAT addresses** field, type the IPv6 SNAT address.
    - In both the **IPv4 SNAT addresses** and **IPv6 SNAT addresses** fields, type both the IPv4 and IPv6 SNAT addresses.
17. From the **Should traffic go to the Internet via specific gateways?** list, select whether or not you want the system to let all SSL traffic use the default route, or if you want to specify Internet gateways (routers). If you chose to use specific gateways, you can also define the ratio of traffic sent to each device in the next step.

- If you want outbound/Internet traffic out using the default route on the BIG-IP system, select **No, send outbound/Internet traffic via the default route** and proceed to step 19 to save.
- If you want to define a list of gateways (routers) to handle outbound SSL traffic (and control the share of traffic each is given), use **Yes, send outbound/Internet traffic via specific gateways** and proceed to step 18.

18. Options to provide the outbound gateway addresses will vary, whether you selected **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**. Specify one or more Internet gateway addresses (routers) to handle outbound SSL traffic so to control the share of traffic each is given.

    - In the **What are the IPv4 outbound gateway addresses?** field, type the IPv4 gateway addresses. Proceed to step 20 to save.
    - In the **What are the IPv6 outbound gateway addresses?** field, type the IPv6 gateway addresses. Proceed to step 19.
    - In both the **What are the IPv4 outbound gateway addresses?** and **What are the IPv6 outbound gateway addresses?** fields, type both the IPv4 and IPv6 gateway addresses. Proceed to step 19.

    Click the + button to add additional addresses.

    You can enter multiple gateways if you have multiple systems and wish to load balance across them. If you do enter multiple addresses, you can also use the ratio value to control the load balancing. For example, if you have two devices, and one handles twice as much traffic as the other, you can set the ratio to 1 on the smaller device, and 2 on the larger one.

19. In the **Non-public IPv6 networks via IPv6 gateways** field, type the requested IPv6 address if you want to route connections to any non-public IPv6 networks via the IPv6 gateways above. Enter the prefix/mask-length (CIDR) of each network. Non-public IPv6 networks are those outside the 2000::/3 block, such as ULA networks in the fc00::/7 block.
20. Click **Save**.

You have now configured an ingress device and an egress device located on one system.

This describes only the fields, lists, and areas needed to configure an ingress and egress device on one system. You should complete the other areas in General Properties before moving on to create services and service chains.

Configuring an ingress device (for separate ingress and egress devices)

The ingress device is either a device or a Sync-Failover device group where each client sends traffic. The ingress device is one or more ingress VLANs where the clients send traffic. The ingress device decrypts the traffic and then, based on protocol, source, and destination, classifies the traffic and passes each connection for inspection.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. From the **Do you want to setup separate ingress and egress devices with a cleartext zone between them?** list, select **Yes, configure separate ingress and egress BIG-IP devices**.
3. From the **Is this device the ingress or egress device?** list, select **This is the INGRESS device to which clients connect**.
4. In the **What is the EGRESS device Application Service name?** field, type the name of the device service.
5. In the **What is the IP address of the EGRESS device control-channel virtual server?** field, type the IP address of the service chain control channel virtual server over on the egress device.
6. In the **What IP address should THIS (ingress) device's control-channel virtual server use?** field, type the IP address of the virtual server for the service chain control channel on a VLAN.

7. In the **What is the control-channel pre-shared key?** field, type a pre-shared key (PSK) value to enable cryptographic protection of the service chain control channel between the ingress and egress devices.
8. From the **Which IP address families do you want to support?** list, select whether you want this configuration to **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**.
   If you do not choose to support both address families, you must configure IP addresses in the family you select for all IP address fields in this application. If you choose **Both IPv4 and IPv6**, you can send intercepted IPv6 traffic through an IPv4 Layer 3 service device.
9. From the **Which is the SSL Forward Proxy CA certificate?** list, select the Certificate Authority (CA) certificate that your clients will trust to authenticate intercepted TLS connections.
10. From the **Which is the SSL Forward Proxy CA private key?** list, select the corresponding private key.

    You import the CA certificate and private key while configuring the Setup Wizard. If you did not use the Setup Wizard, you must import a CA certificate before you can use this functionality.
11. In the **What is the private-key passphrase (if any)?** field, type the private-key passphrase.

    If the key does not have a passphrase, leave the field empty.
12. From the Ingress Device Configuration area, for the **Which VLAN(s) will bring client traffic to the transparent proxy?** setting, select one or more VLANs where transparent-proxy ingress traffic will arrive.
13. From the **How should a server TLS handshake failure be handled?** list, select whether you want the connection to fail or bypass the connection.
14. From the **DNS query resolution** list, select whether to permit the system to send DNS queries directly out to the Internet, or specify one or more local forwarding nameservers to process all DNS queries from Herculon SSL Orchestrator.
    - If you select **Send DNS queries directly to nameservers across the internet**, proceed to step 15.
    - If you select **Send DNS queries to forwarding nameservers on the local network**, proceed to step 16.
15. From the **Do you want to configure local/private DNS zones?** list, select whether you do, or do not, want to configure local or private DNS zones.
    - If you select **No, do not configure any local/private DNS zones**, proceed to step 18.
    - If you select **Yes, configure local/private DNS zones**, proceed to step 17.
16. In the **Which local forwarding nameserver(s) will resolve DNS queries from this solution?** field, type the IP address of local nameservers that will resolve all DNS queries from this implementation and click **Add**. Once you have added the necessary nameserver IP addresses, proceed to step 18.
17. In the **List local/private Forward Zones** setting, click **Add** and type the IP address of one or more nameservers.
18. From the **Do you want to use DNSSEC to validate DNS information?** list, select whether you do, or do not, want to use DNSSEC to validate the DNS information.
19. In the Decrypt Zone to Egress Device Configuration area, for **Are there parallel service devices in the decrypt zone?**, select whether you want to send outbound traffic using the BIG-IP® system default route(s) or send outbound traffic through one or more service devices.
    - If the system will send the traffic through its default route to the internet, which must be configured to point to the egress BIG-IP® system, use **No, send outbound traffic via the BIG-IP default route(s)** and proceed to step 22 to save.
    - If your configuration includes any Layer 3 systems in the decrypt zone that must receive the traffic, use **Yes, send outbound traffic via one or more service device(s)** and proceed to step 17.
20. Options to provide the outbound gateway addresses will vary, whether you selected **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**. Type the IP addresses of the inward interface of the first Layer 3 device in the decrypt zone or the decrypt zone gateway.

- In the **What are the IPv4 decrypt zone gateway addresses?** field, type the IPv4 gateway addresses. Proceed to step 22 to save.
- In the **What are the IPv6 decrypt zone gateway addresses?** field, type the IPv6 gateway addresses. Proceed to step 21.
- In both the **What are the IPv4 decrypt zone gateway addresses?** and **What are the IPv6 outbound gateway addresses?** fields, type both the IPv4 and IPv6 gateway addresses. Proceed to step 21.

Click the + button to add additional addresses.

You can enter multiple gateways if you have multiple systems and wish to load balance across them. If you do enter multiple addresses, you can also use the ratio value to control the load balancing. For example, if you have two devices, and one handles twice as much traffic as the other, you can set the ratio to 1 on the smaller device, and 2 on the larger one.

21. In the **What are the Non-public IPv6 networks via IPv6 gateways?** field, type the requested IPv6 address if you want to route connections to any non-public IPv6 networks via the IPv6 gateways above. Enter the prefix/mask-length (CIDR) of each network. Non-public IPv6 networks are those outside the 2000::/3 block, such as ULA networks in the fc00::/7 block.
22. Click **Save**.

You have now configured an ingress device for a system configured for separate ingress and egress devices.

This describes only the fields, lists, and areas needed to configure an ingress device. You should complete the other areas in General Properties before moving on to create services and service chains.

Configuring an egress device (for separate ingress and egress devices)

The egress device is either a device or a Sync-Failover device group that receives traffic after a connection travels through the specified service chain and directs the traffic to the final destination. When users set up separate ingress and egress devices, they send each other control messages. These can go through the decrypt zone, or around it if you configure a different path through the network. In either case, the messages are sent through TCP connections to port `245`, at an IP address users specify, on each BIG-IP® system.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. From the **Do you want to setup separate ingress and egress devices with a cleartext zone between them?** list, select **Yes, configure separate ingress and egress BIG-IP devices**.
3. From the **Is this device the ingress or egress device?** list, select **This is the EGRESS device to which connects to server**.
4. In the **What is the INGRESS device Application Service name?** field, type the name of the device service.
5. In the **What is the IP address of the INGRESS device control-channel virtual server?** field, type the IP address of the service chain control channel virtual server over on the egress device.
6. In the **What IP address should THIS (egress) device's control-channel virtual server use?** field, type the IP address of the virtual server for the service chain control channel on a VLAN.
7. In the **What is the control-channel pre-shared key?** field, type a pre-shared key (PSK) value to enable cryptographic protection of the service chain control channel between the ingress and egress devices.
8. From the **Which IP address families do you want to support?** list, select whether you want this configuration to **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**.

If you do not choose to support both address families, you must configure IP addresses in the family you select for all IP address fields in this application. If you choose **Both IPv4 and IPv6**, you can send intercepted IPv6 traffic through an IPv4 Layer 3 service device.

9. From the **Which is the SSL Forward Proxy CA certificate?** list, select the Certificate Authority (CA) certificate that your clients will trust to authenticate intercepted TLS connections.
10. From the **Which is the SSL Forward Proxy CA private key?** list, select the corresponding private key.

    You import the CA certificate and private key while configuring the Setup Wizard. If you did not use the Setup Wizard, you must import a CA certificate before you can use this functionality.
11. In the **What is the private-key passphrase (if any)?** field, type the private-key passphrase.

    If the key does not have a passphrase, leave the field empty.
12. From the Egress Device Configuration area, in the **Which VLAN(s) are part of the decrypt zone? (These bring traffic from the ingress device)** setting, select one or more VLANs where transparent-proxy egress traffic will arrive.
13. From the **Do you want to SNAT client IP addresses?** list, select whether you do, or do not, want to define SNAT addresses.
    - If you select **No, pass client addresses unaltered**, proceed to step 16.
    - If you select **Yes, SNAT (replace) client addresses**, proceed to step 14.
14. From the **Do you want to use a SNAT Pool?** list, select whether you want to use a SNAT pool or SNAT auto map to translate addresses.
    - If you select **Yes, define SNAT Pool addresses for good performance**, proceed to step 15.
    - If you select **No, use SNAT Auto Map (not recommended)**, proceed to step 16.
15. Options to provide SNAT addresses will vary, whether you selected **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**. Type at least as many IP host addresses as the number of TMM instances on the ingress device. Each address must be uniquely assigned and routed to the ingress device. It is best to assign addresses which are adjacent and grouped under a CIDR mask, for example, 203.0.113.8 up through 203.0.113.15 which fill 203.0.113.8/29.
    - In the **IPv4 SNAT addresses** field, type the IPv4 SNAT address.
    - In the **IPv6 SNAT addresses** field, type the IPv6 SNAT address.
    - In both the **IPv4 SNAT addresses** and **IPv6 SNAT addresses** fields, type both the IPv4 and IPv6 SNAT addresses.
16. From the **Should traffic go to the Internet via specific gateways?** list, select whether you want the system to let all SSL traffic use the default route, or if you want to specify Internet gateways (routers). If you chose to use specific gateways, you can also define the ratio of traffic sent to each device in the next step.
    - If you want outbound/Internet traffic out using the default route on the BIG-IP system, use **No, send outbound/Internet traffic via the default route** and proceed to step 19.
    - If you want to define a list of gateways (routers) to handle outbound SSL traffic (and control the share of traffic each is given) use **Yes, send outbound/Internet traffic via specific gateways**, proceed to step 17.
17. Options to provide the outbound gateway addresses will vary, whether you selected **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**. Type the IP addresses of the inward interface of the first Layer 3 device in the decrypt zone or the decrypt zone gateway.
    - In the **What are the IPv4 outbound gateway addresses?** field, type the IPv4 gateway addresses. Proceed to step 22 to save.
    - In the **What are the IPv6 outbound gateway addresses?** field, type the IPv6 gateway addresses. Proceed to step 18.

- In both the **What are the IPv4 outbound gateway addresses?** and **What are the IPv6 outbound gateway addresses?** fields, type both the IPv4 and IPv6 gateway addresses. Proceed to step 18.

Click the + button to add additional addresses.

You can enter multiple gateways if you have multiple systems and wish to load balance across them. If you do enter multiple addresses, you can also use the ratio value to control the load balancing. For example, if you have two devices, and one handles twice as much traffic as the other, you can set the ratio to 1 on the smaller device, and 2 on the larger one.

18. In the **Non-public IPv6 networks via IPv6 gateways** field, type the requested IPv6 address if you want to route connections to any non-public IPv6 networks via the IPv6 gateways above. Enter the prefix/mask-length (CIDR) of each network. Non-public IPv6 networks are those outside the 2000::/3 block, such as ULA networks in the fc00::/7 block.
19. In the Decrypt Zone to Ingress Device Configuration area, for **Are there parallel service devices in the decrypt zone?**, select whether you want to send outbound traffic using the BIG-IP system default route(s) or send outbound traffic through one or more service devices.
    - If the system will send the traffic through its default route, which must be configured to point to the ingress BIG-IP system, use **No, send outbound traffic via the BIG-IP default route(s)** and proceed to step 22 to save.
    - If your configuration includes any Layer 3 systems in the decrypt zone that must receive the responses to traffic, use **Yes, send outbound traffic via one or more service device(s)** and proceed to step 20.
20. Options to provide the outbound gateway addresses will vary, whether you selected **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**. Type the IP addresses of the inward interface of the first Layer 3 device in the decrypt zone or the decrypt zone gateway.
    - In the **What are the IPv4 decrypt zone gateway addresses?** field, type the IPv4 gateway addresses. Proceed to step 22 to save.
    - In the **What are the IPv6 decrypt zone gateway addresses?** field, type the IPv6 gateway addresses. Proceed to step 21.
    - In both the **What are the IPv4 decrypt zone gateway addresses?** and **What are the IPv6 outbound gateway addresses?** fields, type both the IPv4 and IPv6 gateway addresses. Proceed to step 21.

    Click the + button to add additional addresses.

    You can enter multiple gateways if you have multiple systems and want to load balance across them. If you do enter multiple addresses, you can also use the ratio value to control the load balancing. For example, if you have two devices, and one handles twice as much traffic as the other, you can set the ratio to `1` on the smaller device, and `2` on the larger one.
21. In the **What are the intranet networks (subnets)?** field, type the IP address and mask-length in CIDR format for intranet submasks.

    Click the + button to add additional addresses. Typical IPv4 entries include `10.0.0.0/8`, `172.16.0.0/12`, and `192.168.0.0/16`.
22. Click **Save**.

You have now configured an egress device for a system configured for separate ingress and egress devices.

This describes only the fields, lists, and areas needed to configure an egress device. You should complete the other areas in General Properties before moving on to create services and service chains.

Configuring the system for transparent proxy

You can configure Herculon SSL Orchestrator to operate in transparent proxy mode only. A *transparent proxy* intercepts normal communication without requiring any special client configuration, so clients are unaware of the proxy in the network.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. From the **Which IP address families do you want to support?** list, select whether you want this configuration to **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**.
   If you do not choose to support both address families, you must configure IP addresses in the family you select for all IP address fields in this application. If you choose **Both IPv4 and IPv6**, you can send intercepted IPv6 traffic through an IPv4 Layer 3 service device.
3. From the **Which proxy schemes do you want to implement?** list, select **Implement transparent proxy only**.
4. From the **Do you want to pass UDP traffic through the transparent proxy unexamined?** list, select one of the options:
   - Use **Yes, pass all UDP traffic unexamined** to pass UDP traffic through without inspecting it.
   - Use **No, manage UDP traffic by classification** to configure specific service chain classifier rules for UDP traffic.
5. From the **Do you want to pass non-TCP, non-UDP traffic through the transparent proxy?** list, select one of the options:
   - Use **Yes, pass non-TCP, non-UDP traffic** (such as IPsec, SCTP, OSPF, and so on) if you want the system to pass all traffic that is not TCP or UDP through the transparent proxy. If you choose this option, this traffic will not be classified or processed by any service chain.
   - Use **No, block all non-TCP, non-UDP traffic** (such as IPsec, SCTP, OSPF, and so on) for the system to block all non-TCP and non-UDP traffic.
6. Click **Save**.

You have now configured Herculon SSL Orchestrator to work in transparent proxy mode.

This describes only the fields, lists, and areas needed to configure Herculon SSL Orchestrator to work in transparent proxy mode. You should also complete the other areas in General Properties before moving on to create services and service chains.

Configuring the system for explicit proxy

You can configure Herculon SSL Orchestrator to operate in explicit proxy mode only. Explicit proxy in Herculon SSL Orchestrator requires manual configuration of the client and supports only HTTP(S) based on RFC2616.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. From the **Which IP address families do you want to support?** list, select whether you want this configuration to **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**.
   If you do not choose to support both address families, you must configure IP addresses in the family you select for all IP address fields in this application. If you choose **Both IPv4 and IPv6**, you can send intercepted IPv6 traffic through an IPv4 Layer 3 service device.
3. From the **Which proxy schemes do you want to implement?** list, select **Implement explicit proxy only**.

4. In the Explicit Proxy Configuration area, from the **On which VLAN(s) should the explicit proxy listen?** field, select one or more BIG-IP® VLANs where the explicit proxy listens.
5. Options to provide the outbound gateway addresses will vary, whether you selected **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**. Type the IP address and port that the BIG-IP system should use for the explicit proxy virtual server using one of these options.
   - In the **What IPv4 address and port should the explicit proxy use?** field, type the IPv4 address and port.
   - In the **What IPv6 address and port should the explicit proxy use?** field, type the IPv6 address and port.
   - In both the **What IPv4 address and port should the explicit proxy use?** and **What IPv6 address and port should the explicit proxy use?** fields, type both the IPv4 and IPv6 address and port information.
6. Click **Save**.

You have now configured Herculon SSL Orchestrator to work in explicit proxy mode.

This describes only the fields, lists, and areas needed to configure Herculon SSL Orchestrator to work in explicit proxy mode. You should also complete the other areas in General Properties before moving on to create services and service chains.

Configuring the system for both transparent and explicit proxies

Explicit proxy in Herculon™ SSL Orchestrator requires manual configuration of the client and supports only HTTP(S) based on RFC2616.

You can configure Herculon SSL Orchestrator to operate in transparent and explicit proxy mode. A *transparent proxy* intercepts normal communication without requiring any special client configuration, so clients are unaware of the proxy in the network.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. Scroll down to the **Which IP address families do you want to support?** list, and select whether you want this configuration to **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**.
   If you do not choose to support both address families, you must configure IP addresses in the family you select for all IP address fields in this application. If you choose **Both IPv4 and IPv6**, you can send intercepted IPv6 traffic through an IPv4 Layer 3 service device.
3. From the **Which proxy schemes do you want to implement?** list, select **Implement both transparent and explicit proxies**.
4. From the **Do you want to pass UDP traffic through the transparent proxy unexamined?** list, select one of the options:
   - Use **Yes, pass all UDP traffic unexamined** to pass UDP traffic through without inspecting it.
   - Use **No, manage UDP traffic by classification** to configure specific service chain classifier rules for UDP traffic.
5. From the **Do you want to pass non-TCP, non-UDP traffic through the transparent proxy?** list, select one of the options:
   - Use **Yes, pass non-TCP, non-UDP traffic** (such as IPsec, SCTP, OSPF, and so on) if you want the system to pass all traffic that is not TCP or UDP through the transparent proxy. If you choose this option, this traffic will not be classified or processed by any service chain.
   - Use **No, block all non-TCP, non-UDP traffic** (such as IPsec, SCTP, OSPF, and so on) for the system to block all non-TCP and non-UDP traffic.
6. In the Explicit Proxy Configuration area, from the **On which VLAN(s) should the explicit proxy listen?** field, select one or more BIG-IP® VLANs where the explicit proxy listens.

7. Options to provide the outbound gateway addresses vary, whether you selected **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**. Type the IP address and port that the BIG-IP system should use for the explicit proxy virtual server, using one of these options.
   - In the **What IPv4 address and port should the explicit proxy use?** field, type the IPv4 address and port.
   - In the **What IPv6 address and port should the explicit proxy use?** field, type the IPv6 address and port.
   - In both the **What IPv4 address and port should the explicit proxy use?** and **What IPv6 address and port should the explicit proxy use?** fields, type both the IPv4 and IPv6 address and port information.

You have now configured Herculon SSL Orchestrator to work in both transparent and explicit proxy modes.

This describes only the fields, lists, and areas needed to configure Herculon SSL Orchestrator to work in both transparent and explicit proxy modes. You should also complete the other areas in General Properties before moving on to create services and service chains.

Creating Services, Service Chains, and Classifier Rules

Overview: Creating services, service chains, and classifier rules

This section decribes how to create inline services, ICAP services, receive-only services, service chains, and classifier rules.

Creating inline services for service chains

Before creating inline services, complete all areas in General Properties. Refer to the *Configuring general properties* section of this document for more information.

Inline services pass traffic through one or more service devices at Layer 2 or Layer 3. You use inline services in service chains, where each service device communicates with the BIG-IP® device, on the ingress side and over two VLANs. These VLANs route traffic toward the intranet and Internet, respectively.

Layer 3 inline services requires you to provide the IP address of the service devices from the present choices in the Herculon SSL Orchestrator configuration. If you are using Layer 3 inline services, this configuration sends and receives information from the services using a pre-defined set of addresses.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Services** > **Inline Services** to view inline services settings.
   The Inline Services screen opens.
2. Options to provide the IPv4 (CIDR/19) subnet-block base address, the IPv6 /48 subnet-block prefix, or both, will vary, whether you selected **Support IPv4 only**, **Support IPv6 only**, or **Both IPv4 and IPv6**.
   - In the **What is the IPv4 (CIDR/19) subnet-block base address?** field, type the address block. F5 recommends the default block `198.19.0.0/19` to minimize the likelihood of address collisions.

     Note: *When using Layer 3 inline services, you must address your systems to match the required ranges. Even though you can change the base address of each address block (IPv4) from which subnets and addresses are assigned, changing an address block has several implications, must be done with caution, and is not recommended or supported by F5.*
   - In the **What is the IPv6 /48 subnet-block prefix?** field, type the address block.

     Note: *Each inline service goes through one or more services at Layer 2 (LAN) or Layer 3 (IP). Each service device communicates with the BIG-IP device on the ingress side over two VLANs (from BIG-IP and to BIG-IP) that carry traffic toward the intranet and the internet, respectively.*
   - In both the **What is the IPv4 (CIDR/19) subnet-block base address?** and **What is the IPv6 /48 subnet-block prefix?** fields, type the necessary address block information.
3. Click **Add**.
4. In the **Name** field, type a name for your configuration.

   Use a short, unique name for this service. This name can contain 1 -15 alphanumeric or underscore characters, but must start with a letter. Letters are not case-sensitive.
5. From the **Service Type** list, select **Layer 2** or **Layer 3**.
6. In the **Interfaces** area, select the BIG-IP system interface and VLAN tag for each VLAN pair.

Each Inward VLAN must be connected to the same Layer 2 virtual network from every device in the Sync-Failover Device Group, and each Outward VLAN likewise, but to a distinct Layer 2 virtual network.

If you choose to use the **Ratio** field, the BIG-IP system distributes connections among pool members in a static rotation according to ratio weights that you define. In this case, the number of connections that each system receives over time is proportionate to the ratio weight you defined for each pool member or node. This number must be between 1-100.

For example, if you have five devices and you assign a ratio of **1** to the first three devices, and a ratio of **2** to the fourth device, and a ratio of **3** to the fifth device; the first three devices with a ratio of 1 each receive 1/8 of the traffic. The fourth device receives 1/4 of the traffic, and the fifth device receives 3/8 of the traffic.

7. Under Available Devices, from the **IP Address** list, select the IP address pairs of the Layer 3 devices and click **Add** to add them to the **IP Address** field.
8. From the **Translate Port for HTTP Traffic** list, select one of the options.
   - Use **No** if the connections should use their original destination ports.
   - Use **Yes to Port 80** to send all HTTP traffic through port 80.
   - Use **Yes to Port 8080** to send all HTTP traffic through port 8080.
   - Use **Yes to Port 8443** to send all HTTP traffic through port 8443.
9. From the **Connection Handling On Outage** list, select one of the following:
   - Use **Skip Service** to allow connections to skip the service you are configuring if all the devices in the service are unavailable.
   - Use **Reject Connection** for the system to reject every connection reaching the service when the service is down.
10. Click **Finished**.
11. Click **Save**.

Note:

Layer 3 devices need to follow a specific fixed addressing scheme. For each of the 10 possible Layer 3 inline services, you need to use the following configuration (with **x** being 0-9 representing the inline service):

Inward Interface:

- IPv4 Address: `198.19.x.61` through `68` (for each of the load balanced Layer 3 devices)
- IPv4 Netmask: `255.255.255.128`
- IPv6 Address: `fd06:4d61:x::41` through `48` (for each of the load balanced Layer 3 devices)
- IPv6 Netmask: `ffff.ffff. ffff.ffff. ffff.ffff. ffff.ff00`

Outward Interface:

- IPv4 Address: `198.19.x.161` through `168` (for each of the load balanced Layer 3 devices)
- IPv4 Netmask: `255.255.255.128`
- IPv6 Address: `fd06:4d61:x::141` through `148` (for each of the load balanced Layer 3 devices)
- IPv6 Netmask: `ffff.ffff. ffff.ffff. ffff.ffff. ffff.ff00`

Routes:

- Default Gateway: `198.19.x.245`
- Gateway to internal networks: `.1`

While the base address can be changed if needed, F5 recommends leaving it set to the default: `198.19.0.0`.

You have now configured an inline service for Herculon SSL Orchestrator.

After creating more than one service, you can now create a service chain.

Creating ICAP services

Before creating ICAP services, complete all areas in General Properties. Refer to the *Configuring general properties* section of this document for more information.

ICAP services use the RFC3507 ICAP protocol to refer HTTP traffic to one or more content adaptation devices to inspect or modify. You can add an ICAP to any TCP service chain, but only HTTP traffic is sent to the chain. Additionally, you can configure up to ten ICAP services using the Herculon SSL Orchestrator configuration utility to load balance across them.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Services** > **ICAP Services** to view ICAP services settings.
   The ICAP Services screen opens.
2. Click **Add**.
3. In the **Name** field, type a name for your configuration.
4. In the **ICAP Devices** field, type an IP address and port number and click **Add**.
5. For **Headers**, from the **Mode** list, select either **Default** or **Custom**.

   To edit the headers, use **Custom**.
6. From the **TCP Connections** list, select F5®**OneConnect™** or **Separate**.

   Use **OneConnect** to reuse the TCP connections to ICAP servers, which processes multiple transactions. If your ICAP servers do not support multiple ICAP transactions per TCP connection, select **Separate**. OneConnect will then be disabled.
7. From the **Type** list, select either **Load Balanced** or **Custom**.
   - If you select **Load Balanced**, the **Request** and **Response** fields are prepopulated with keywords that will be automatically replaced by the configured active ICAP server and port at the time of the request. The specific page name for the request and response must be manually entered to complete the URI. For example, if the request URI for the ICAP servers will be “icap://10.1.2.3:1344/REQ”, you enter “REQ” in the request field.
   - If you select **Custom**, the **Request** and **Response** fields are empty and the entire URI content must be manually entered. In this case, Herculon SSL Orchestrator will not load balance traffic across the configured ICAP servers. For example, if the request URI for the ICAP server will be “icap://icap.example.com/request”, you enter the entire URI into the request field.
8. In the **Request** and **Response** fields, type the ICAP request and response URI, defined by RFC3507, that are related to the ICAP server and based on whether you selected **Load Balanced** or **Custom** in the previous step.
9. In the **Preview Max. Length (bytes)** field, type the number of bytes that are in the maximum length for the ICAP preview.

   Bytes of content, up to the specified number, are sent to the ICAP server as a preview of each HTTP request or response. If you set the maximum preview length to zero (0), then requests and responses are streamed through the ICAP server. The largest value currently supported is 51200 (50KB).
10. From the **Server Failure Handling** list, select **Reset Connection** or **Next Service Chain**.
    - Use **Reset Connection** for the system to reset the connection to the client, discarding the request and response.
    - Use **Next Service Chain** for the system to let the request or response continue to the next service in the service chain.
11. From the **Send HTTP/1.0 Requests to ICAP** list, select how to send requests to the ICAP service.
    - Use **HTTP/1.0 & HTTP/1.1** to send both HTTP/1.0 and HTTP/1.1 requests to the ICAP service.

- Use **HTTP/1.1 only** to send only HTTP/1.1 requests to the ICAP service. Any HTTP/1.0 requests are not inspected.

12. Click **Finished**.
13. Click **Save**.

You have now configured an ICAP service.

After creating more than one service, you can now create a service chain.

Creating receive-only services for traffic inspection

Before configuring receive-only services, complete all areas in General Properties. Refer to the *Configuring general properties* section of this document for more information.

Receive-only services only receive traffic for inspection and do not send the traffic back to the BIG-IP® system. Each receive-only service provides a packet-by-packet copy of the traffic passing through the service to an inspection device. You can configure up to ten receive-only services using the F5® Herculon™ SSL Orchestrator™ configuration utility.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Services** > **Receive Only Services** to view receive-only services settings.
   The Receive Only Services screen opens.
2. Click **Add**.
3. In the **Name** field, type a name for your configuration.
4. In the **MAC Address** field, type the MAC address of the receive-only device.
5. In the **IP Address** field, type the nominal IP address for this device.

   Each receive-only device requires a nominal IP host address to identify the device in the BIG-IP system.
6. From the **VLAN** list, select the VLAN where the receive-only device resides.
7. From the **Interface** list, select the associated BIG-IP system interface.
8. Click **Finished**.
9. Click **Save**.

You have now created a receive-only service for Herculon SSL Orchestrator.

After creating more than one service, you can now create a service chain.

Creating service chains to link services

Before you can set up service chains, you must configure multiple services such as inline, ICAP, or receive-only.

You can create service chains using previously-created services. A *service chain* is a list of services linked to service chain classifier rules. Service chains process specific connections based on classifier rules that look at protocol, source, and destination addresses. Additionally, service chains can include the following types of services, as well as any decrypt zones between separate ingress and egress devices:

- Layer 2 inline services
- Layer 3 inline services
- Receive-only services
- ICAP services

1. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Policies** to view service chain settings.
   The Service Chain information on the Policies screen opens.
2. Click **Add**.
3. In the **Name** field, type a name for your service chain.

   Create a short name for this service chain. A service chain name may contain 1-15 alphanumeric or underscore characters and must start with a letter (not case-sensitive). Use spaces or commas to separate service names.

   Note: *You cannot use any of the keywords "all", "bypass", "reject", or "drop", nor the name of any (inspection) service you previously configured as a service chain name.*
4. In the **Services** area, select a **Type** and **Name** and then click **Add**.
5. Click **Finished**.
6. Click **Save**.

You have now configured a service chain.

After you create a service chain, configure either TCP or UDP classifier rules.

Creating TCP service chain classifier rules

Before you create a TCP service chain classifier rule, you must create one or more service chains.

Service chain classifier rules determine which service chains receive traffic. Each service chain classifier rule you choose selects the specific chain to process ingress connections. Different classifier rules can send connections to the same chain. Each classifier has three filters that match the source IP address, the destination, and the application protocol. Filters can also overlap, so the best matching classifier determines the service chain for a specific connection, and classifiers can reject a connection or allow it to bypass the service chain. In addition, you can also choose to send decrypted or non-decrypted traffic to the inspection devices.

Note: *When configuring a single device Herculon SSL Orchestrator transparent proxy in front of an explicit proxy, Herculon SSL Orchestrator can transparently intercept SSL traffic tunneled through an explicit proxy and selectively forward the decrypted user traffic through the security service chain for proper inspections. Afterwards, the user traffic is sent back to the BIG-IP, which re-encrypts the traffic and sends to the explicit proxy. User traffic of certain categories may also be rejected by the BIG-IP or bypass the security inspections.*

Note: *When transparently decrypting traffic to upstream explicit proxies in a two device Herculon SSL Orchestrator deployment, the SSL forward proxy interception only occurs on the ingress device (decryption, service chaining, and re-encryption occur on the ingress device, while the encrypted plaintext traffic will pass through the egress device). In addition, all classifier rules apply to traffic inside HTTP CONNECT tunnels except for rules bypassing SSL during the TLS handshake phase. Rules bypassing SSL during the TLS handshake phase do not apply because SSL forward proxy cannot reuse the same HTTP CONNECT tunnel to the explicit proxy for the bypassed flow.*

1. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Policies** to view TCP service chain classifiers settings.
   The TCP Service Chain Classifiers information on the Policies screen opens.
2. In the TCP Service Chain Classifiers area, click **Add**.
3. In the **Name** field, type a name for this rule.
4. From the **Phase** list, select a phase for this classifier.

- Use **Normal** if the rule may match TLS connections at TLS handshake time and possibly again, more specifically, after Herculon SSL Orchestrator exposes the plaintext of the TLS connection (so you can manage HTTPS on nonstandard ports, for example). Normal rules may also match non-TLS traffic (so, for example, a single rule can handle both HTTPS and HTTP).
- Use **No TLS** if the rules match only non-TLS traffic.
- Use **Pre Handshake** to have the rules match before any TLS handshake. This means the rules can allow a connection to bypass SSL inspection completely,without even trying to learn the real name of the remote server. All Dynamic Domain Bypass (DDB) rules must have **Phase** set to **Pre Handshake**.
- Use **TLS Handshake** rules to have the rules match only at TLS handshake time: they will never match non-TLS traffic, and they are not checked again after the plaintext of a TLS connection becomes available.

5. From the **Protocol** list, select the protocol of the connection based on the port number or protocol recognition.
6. In the **Source** area, select a **Type** and a **Value**.

   This option specifies the name of the Service Chain you configured that you want to use for this classifier rule. From the **Type** list, select one of the following and then click **Add**.

   - For **IP Address**, type the required IP address in the **Value** field.
   - For **Data Group**, select the name of your data group from the **Value** list.
7. In the **Destination** setting, select a **Mode**, **Type**, and **Value**.

   This option specifies the destination of the connection. The value of this field is based on the selection you made for the mode.

   - From the **Mode** list, select the mode you want to use for this classifier rule. The mode you choose determines the value you will use for the destination. You can choose one of the modes for each classifier rule:
     - For **Address**, the **Destination** filter you configure consists of one or more IP subnet or host addresses just like the **Source** filter.
     - For **Geolocation**, the **Destination** you configure contains 2-letter country and 3-letter continent codes against which the IP Geolocation of the destination server is compared. The continent codes are: **CAF**=Africa, **CAN**=Antarctica, **CAS**=Asia, **CEU**=Europe, **CNA**=North America, **COC**=Oceania, **CSA**=South. The country codes are those of ISO 3166 alpha-2.
     - For **IPI** (IP Inspection), the **Destination** you configure contains one or more IP Intelligence categories against which the destination IP address's reputation is matched. You must replace SPACE characters in names of IP Intelligence categories with underscores (_) before adding them to **Destination**.
     - For **Port**, the **Protocol** value must be **All**. The **Destination** contains one or more TCP port numbers or ranges like 5557-5559 (use 0 or * to match all) against which the destination port number is matched. The main use of this mode is to control non-TLS traffic such as SSH.
     - For **URLF** (URL Filtering), the **Destination** you configure is one or more URL Filtering categories against which the URL categorization of the destination server is compared. You must replace SPACE characters in names of URL Filtering categories with underscores (_) before adding them to **Destination**.
     - For **DDB** (Dynamic Domain Bypass), the **Destination** you configure contains one or more DNS domain names (unique or wildcard) against which the destination hostname indicated by the client in TLS SNI is matched. This mode is special because it classifies traffic before the Herculon SSL Orchestrator implementation attempts any TLS handshake with the remote server (that is, in Match Phase Pre-handshake). You may use **DDB** to whitelist and bypass traffic to servers which cause TLS handshake problems or that require TLS mutual (client-certificate/smart-card) authentication. For **DDB**, the **Service Chain** value you select must be **Bypass** or **Reject**.

For security, the DDB facility ensures the destination IP address for each bypassed connection corresponds to the allowed domain. DDB may replace the destination IP address supplied by the client with one freshly obtained from DNS.

- For **Name** (domain name), the **Destination** you will configure contains one or more DNS domain names (unique or wildcard) against which the connection's destination host name is matched.

- From the **Type** list, depending on which **Mode** you selected, choose either **IP Address**, **Data Group**, **Category**, or **Domain Name** (or there will be no selection required).
- From the **Value** list or field, depending on which **Type** and **Mode** you selected, choose a value from the list or type in the required information (hover your mouse over the field for tips on required information).

8. Click **Add**.
9. From the **Service Chain** list, select the name of the service chain you configured that you want to use for this classifier rule. This must be the name you gave a service chain or a special keyword:

   - **All** means a chain including all services: first receive-only services, then ICAP services, then in-line services.
   - **Reject** terminates the connection.
   - **Bypass** lets the connection go to its destination without traversing any service chain.

   By specifying service chain classifier rules, if more than one classifier matches a connection, the best-matching classifier determines the service chain for that connection (so the order of classifier rules in the list is not important). Classifiers can also reject a connection or let it bypass the service chain (bypass TLS interception). The default action applies to connections which do not match any classifier.

   This classifier is the element of the Herculon SSL Orchestrator implementation which selects the proper service chain to handle each connection. A *connection*" is a particular packet flow between client (source) and server (destination), identified by the 5-tuple of IP protocol (TCP or UDP), plus client (source) and server (destination) IP addresses and port numbers. The classifier has a set of rules for TCP connections, and another set of rules for UDP when UDP service chains are enabled. The classifier matches information describing each connection, such as its client and server IP addresses, against criteria specified in the classifier rules. For example, a classifier rule might match all connections from clients homed on a certain IP subnet. Another classifier rule might match all connections going to servers in a certain country (using IP Geolocation).
10. To bypass decryption and send encrypted traffic to inspection devices, deselect the **Decrypt** check box. By default, the **Decrypt** check box is turned on and cannot be changed unless you have set the Phase field to **Pre Handshake** and the Service Chain classifier to **All**.

    Note: *If you have upgraded to a new Herculon SSL Orchestrator version, or are using a previous configuration, the* ***Decrypt*** *check box is selected by default.*

    ---

11. Click **Finished**.
12. From the **What should happen to unmatched connections?** list, select how the system should handle unmatched connections.
13. Click **Save**.

You have now created a TCP service chain classifier rule.

Creating UDP service chain classifier rules

Before you create a UDP service chain classifier rule, you must create one or more service chains.

Service chain classifier rules determine which service chains receive traffic. Each service chain classifier rule selects the specific chain to process ingress connections. Different classifier rules may send connections to the same chain. Each classifier has three filters that match the source IP address, the

destination, and the application protocol. Filters can also overlap, so the best matching classifer determines the service chain for a specific connection. Finally, classifiers can reject a connection or allow it to bypass the service chain.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Policies** to view UDP service chain classifiers settings.
   The UDP Service Chain Classifiers information on the Policies screen opens.
2. In the UDP Service Chain Classifiers area, click **Add**.
3. In the **Name** field, type a name for this rule.
4. From the **Protocol** list, select the protocol of the connection based on the port number or protocol recognition.
5. In the **Source** area, select a **Type** and type a **Value**.

   This option specifies the name of the Service Chain you configured that you want to use for this classifier rule.
6. In the **Destination** area, select a **Mode** and **Type**, and type a **Value**.

   This option specifies the destination of the connection. The value of this field is based on the selection you made for the mode.
7. From the **Service Chain** list, select **All**.
8. Click **Finished**.
9. From the **What should happen to unmatched connections?** list, select how the system should handle unmatched connections.
10. Click **Save**.

You have created a UDP Service Chain Classifier rule.

Importing and Exporting Configurations for Deployment

Overview: Importing and exporting configurations for deployment

You can use F5® Herculon™ SSL Orchestrator™ to both import and export previously successful configurations to resolve specific configuration deployment issues or deploy into any Herculon SSL Orchestrator environment. By importing new configurations, you can use external configuration JSON (JavaScript®Object Notation) files to reset your Herculon SSL Orchestrator settings. When importing past configurations, you can use the roll back capability by selecting a previously saved or imported file from a list that also contains user-specified comments. By rolling back to a previously successful deployment configuration, you can quickly resolve specific configuration issues in a current deployment, or fix a corrupted environment.

You can also export previously successful deployment configurations as JSON files to use in any Herculon SSL Orchestrator environment. These exported configurations can be used to address other specific configuration issues.

Importing new configurations for deployment

Before you import new configurations for deployment, complete all areas in General Properties. Refer to the *Configuring general properties* section of this document for more information.

You can import previously successful configuration JSON files, and examine any differences between the current configuration and the imported configuration prior to deployment.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Settings** > **Import Configs** to view import configuration settings.
   The Import Configurations screen opens.
2. From the **Import Configurations From** list, select **File**.
3. Click **Choose File** and select the location of the configuration JSON file saved on your local system that you want to import.
4. Select the JSON file and click **Open**.
   The JSON file you selected opens next to the **Choose File** button. If the file contains the correct structure, the **Update** button is enabled.
5. Click **Update**.
   If the file's configuration has been altered, a dialog box opens asking if you want to continue importing the file.
6. Specify what you want to do.
   - To examine the differences between the current configuration and the imported configuration, click **OK**.
   - To stop the import process, click **Cancel**.

   If you clicked **OK**, an automatically generated JSON dialog box opens asking `Do you wish to import these SSL Orchestrator configuration settings?`. The current configuration and the imported configuration display next to each other, and show any configuration differences that might be found between the two files. Make sure to review all of the differences between the two files to verify that this is the configuration you want to import.
7. To import the contents of the configuration file, click **OK**, or click **Cancel** to stop the import process.
8. Click **Deploy** to deploy the imported configuration into Herculon SSL Orchestrator.
9. Click **Finished**.

You have now imported a new configuration into Herculon SSL Orchestrator.

Importing past configurations for deployment

Before you import past configurations for deployment, complete all areas in General Properties. Refer to the *Configuring general properties* section of this document for more information.

Before deploying a configuration, you can roll back to previously successful deployment configurations and examine any differences between the current configuration and the past configuration.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Settings** > **Import Configs** to view import configuration settings.
   The Import Configurations screen opens.
2. From the **Import Configurations From** list, select **Past Deployment**.
   The screen lists previously saved deployments.
3. Select a previously saved configuration to import.
4. Click **Update**.
   An automatically generated JSON dialog box opens, asking `Do you wish to rollback your SSL Orchestrator configuration settings?`. The current configuration and the past configuration display next to each other, and show any configuration differences that might be found between the two files. Make sure to review all of the differences between the two files to verify that this is the configuration you want to import.
5. To import the contents of the past deployment, click **OK**, or click **Cancel** to stop the import process.
6. Click **Deploy** to deploy the past configuration into Herculon SSL Orchestrator.
   A Deploy Comments popup dialog box opens where you can enter information specific to the successfully deployed past configuration.

You have now deployed a past configuration into Herculon SSL Orchestrator.

Exporting configurations for deployment

Before you export configurations for deployment, complete all areas in General Properties. Refer to the *Configuring general properties* section of this document for more information.

You can export previously successful deployment configurations as JSON files and examine configuration settings prior to exporting it to your local system. Exported JSON files can later be imported and used to deploy configurations in other Herculon™ SSL Orchestrator environments.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**, and on the menu bar, click **Settings** > **Export Configs** to view export configuration settings.
   The Export Configurations screen opens.

   Note: *If you do not have any previously saved deployments, no information displays.*

2. From the Export Configurations table, select a previously deployed configuration.
3. Click **Export**.
   A dialog box popup opens showing the JSON configuration information to be exported, and asks `Do you wish to export the current SSL Orchestrator Configuration settings to a .json file?`.
4. To export the current Herculon SSL Orchestrator settings into a JSON export file, click **OK**, or click **Cancel** to stop the export process.
5. Type the filename of the JSON file to export.
6. Click **OK**.

The configuration information you selected to export is downloaded to your local system as a JSON file, and can be imported and used to deploy configurations in other Herculon SSL Orchestrator environments.

Setting up Herculon SSL Orchestrator in a High Availability Environment

Overview: Setting up Herculon SSL Orchestrator in a high availability environment

This section describes how to deploy F5® Herculon™ SSL Orchestrator™ high availability (HA). Herculon SSL Orchestrator HA configuration and deployment ensures a decrease in downtime and eliminates single points of failure. The deployment of Herculon SSL Orchestrator's HA works with the BIG-IP®device groups support to sync the Herculon SSL Orchestrator specific configuration items, and is transparent to the user.

The deployment occurs after completing a configuration change and selecting Deploy. The deployment request is first routed to one of the devices in the HA device group. This first device configures the device where the request is received. After successful deployment on that device, the request is repeated on other BIG-IP devices.

With Herculon SSL Orchestrator installed onto a dedicated system with failover, it automatically takes over in case of system failure. Data is synchronized between the two systems, ensuring high availability and consistent protection.

Note: *Herculon SSL Orchestrator high availability deployment is supported for use only with the Herculon SSL Orchestrator configuration utility versions 2.1 and later.*

Assumptions and dependencies

To ensure that your Herculon SSL Orchestrator HA deployment succeeds, it is critical that you closely review and follow all assumptions and dependencies.

- HA Setup: BIG-IP HA (CMI) must be set to Active-Standby mode with network failover. See the *BIG-IP Device Service Clustering: Administration* document for detailed information on Active-Standby HA mode.
- HA Setup: If the deployed device group is not properly synced or RPM packages are not properly syncing, make sure your HA self IP (for example, `ha_self`) **Port Lockdown** setting is not set to **Allow None**. On the Main tab, click **Network** > **Self IPs** and click your `ha_self`. If **Port Lockdown** is set to **Allow Custom**, check that the HA network port 443 is open on self IP.
- BIG-IP HA Devices: Only manual sync is supported.
- BIG-IP HA Devices: Devices in each BIG-IP HA pair must be the same model and run the same version of TMOS® (including any hotfixes). Except for the management interface, you must configure both devices to use the same arrangement of network interfaces, trunks, VLANs, self IPs (address and subnet mask), and routes. For example, if one BIG-IP device is connected to a specific VLAN/subnet using interface 1.1, the other BIG-IP device must also be connected to that VLAN/subnet using interface 1.1. If the BIG-IP device configurations do not match, this implementation will not deploy correctly, and HA failover will not work.
- User Experience: Deployment must be initiated from the active HA BIG-IP device.
- User Experience: If the environment is changed from non-HA to HA, or from HA to non-HA, the application must be redeployed.
- User Experience: You can refresh the SSL Configuration screen (**SSL Orchestrator** > **Configuration**) for each peer device in order to see all modified changes.

Task summary for deploying in a high availability environment

To ensure that your F5® Herculon™ SSL Orchestrator™ high availability (HA) deployment succeeds, it is critical that you closely follow each deployment step, as well as the assumptions and dependencies, for both devices in the device group. In addition, you should adhere to all prerequisites. If the systems in the device group are not configured consistently, the deployment synchronization process might suffer errors or fail.

Use the following tasks to ensure your HA deployment succeeds:

- *Installing an updated RPM file*
- *Configuring the network for high availability*
  - *Configuring the ConfigSync and Failover IP address*
  - *Adding a device to the local trust domain*
  - *Creating a Sync-Failover device group*
- *Synchronizing the device group*
- *Setting up a basic configuration for deployment*

Note: *See the Diagnosing your Herculon SSL Orchestrator deployment section for more detailed information on how to monitor the success or failure of your configuration modification.*

Prerequisites

Before configuring the network for high availability, make sure these prerequisites are in place:

- The information used to configure your devices is identical on both devices. Without identical information on both devices, the HA deployment process can suffer from errors or fail.
- The most current RPM file is successfully installed on the first device (the Active device). See the section *Installing an updated RPM file* to ensure that this prerequisite has been properly completed.
- Successfully set up an HA ConfigSync device group prior to starting the configuration. See the section *Configuring the network for high availability* and its subsections to ensure that this prerequisite has been properly completed. For additional information, refer to the *BIG-IP Device Service Clustering: Administration* document, section *Managing Configuration Synchronization*.
- Herculon SSL Orchestrator is installed with the appropriate license information using the Herculon SSL Orchestrator Setup Wizard (or the CLI) and made sure your device setup information is identical on both devices:
  - While using the Herculon SSL Orchestrator Setup Wizard, you have noted the details used for NTP and DNS setup and made sure they will be identical on both devices. To verify duplication, on the Main tab, click **System** > **Configuration** > **Device** and select **NTP** or **DNS**.
  - Ensure that any certificates used in the configuration are copied to all devices.
  - Ensure that information is identical on all devices. This information should include any of the following that are needed:
    - Client network
    - External network
    - Decrypt zone network
    - Decrypt zone control network
    - Networks providing access to ICAP devices and Receive-only devices
  - Ensure that the log publishers are configured and named the same.
  - Ensure that all systems use the same interfaces for any services. (If interface 1.1 is used to send traffic to an inline Layer 2 device on system A, then interface 1.1 must also be used on systems B, C, and D.)

Note: *Do not attempt to duplicate the configuration by saving and restoring a user configuration set (UCS) file from one machine to the other, or any other cloning approach. There are several IDs that must be unique that will also be duplicated, causing additional problems.*

Note: *For more detailed information on using the Herculon SSL Orchestrator Setup Wizard, see the Using the Herculon SSL Orchestrator setup wizard section.*

Installing an updated RPM file

Create a backup of your current configuration to ensure your settings are not lost if the update fails.

Having the latest version of F5® Herculon™ SSL Orchestrator™ establishes the version that later appears on your other BIG-IP® HA peer device. After downloading the latest version of the Herculon SSL Orchestrator zip file from *downloads.F5.com*, return to your Herculon SSL Orchestrator configuration utility.

1. On the Main tab, click **SSL Orchestrator** > **Updates**.
   The Updates screen opens.
2. For the **File Name** setting, click **Browse** and navigate to the file you saved onto your system.
3. Click **Open** to select it.
4. Click **Install**.

Note: *Install the Herculon SSL Orchestrator configuration utility package (the `*.rpg` file) on the active system only. That system will copy it to the other systems in the ConfigSync group.*

Later, after a successful Herculon SSL Orchestrator HA deployment, you should verify that the same version appears on the BIG-IP HA peer device. See the section *Updating the Herculon SSL Orchestrator version* for more detailed installation instructions.

Configuring the network for high availability

You can specify the settings for VLAN HA and self IP addresses on the active device to configure your network for high availability. If needed, you can configure all devices involved in the high availability group for HA.

Note: *This network connects the various devices and must be a common Layer-2 network between all devices.*

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   A New VLAN screen opens where you can configure your new VLAN.
3. In the **Name** field, type the name (for example, `ha_vlan`).
4. For the **Interfaces** setting:
   a) From the **Interface** list, select an interface number.
   b) From the **Tagging** list, select **Tagged** for traffic for that interface to be tagged with a VLAN ID.
   c) Click **Add**.
      The interface you selected appears in the **Interfaces** list as a tagged service.
5. Click **Finished**.
   Next to the F5 logo, your device status appears showing `ONLINE (ACTIVE)` and `Standalone` with green indicators showing their status as up and running.
6. On the Main tab, click **Network** > **Self IPs** .

The Self IP List screen opens.

7. Click **Create**.
   A New Self IP screen opens where you can configure your new self IP.
8. In the **Name** field, type the self IP name (for example, `ha_self`).
9. In the **IP Address** field, type the IP address for the device.
10. In the **Netmask** field, type the netmask for the device.
11. From the **VLAN/Tunnel** list, select the VLAN name (`ha_vlan`).
12. Click **Finished**.

Configuring ConfigSync and failover IP addresses

Before creating the device group, you should configure the configuration synchronization (ConfigSync) and Failover IP addresses for each BIG-IP® system in the device group. The ConfigSync address is the IP address that the system uses when synchronizing configuration with peer devices, and the failover address is the IP address that the system uses for network failover.

1. On the Main tab, click **Device Management** > **Devices**.
   The Devices List screen opens.
2. Click your device in the device list.
   The properties screen for the device opens.
3. Click **ConfigSync**.
   The screen shows the ConfigSync Configuration area, with the local address of the device.
4. From the **Local Address** list, select the VLAN address (`ha_vlan`).
5. Click **Update**.
6. Click **Failover Network**, and then click **Add**.
   The New Failover Unicast Address screen opens.
7. In the **Address** field, make sure that the VLAN address (`ha_vlan`) is present.
8. Click **Repeat**.
9. After the screen refreshes, from the **Address** list, select the Management Address.

Note: *Connection Mirroring is not supported.*

---

10. Click **Finished**.
    The Failover Unicast Configuration area lists both the VLAN HA (`ha_vlan`) and Management Address devices.

Adding a device to local trust domain

Any BIG-IP® devices that you intend to add to a device group must first be members of the same local trust domain. When a BIG-IP device joins the local trust domain, it establishes a trust relationship with peer BIG-IP devices that are members of the same trust domain. For example, if you are creating a device group with two members, you must log in to one of the devices and join the other device to that system's local trust domain. The devices can then exchange their device properties and device connectivity information.

1. On the Main tab, click **Device Management** > **Device Trust**.
   The Device Trust screen opens.
2. On the menu bar, click **Device Trust Members** to view peer and subordinate device settings.
   The Device Trust Members screen opens.
3. Click **Add**.
   The Device Trust screen opens, showing Retrieve Device Credentials (Step 1 of 3).
4. From the **Device Type** list, select **Peer**.
5. In the **Device IP Address** field, type the IP address of your device.

6. Click **Retrieve Device Information**.
   The screen shows Verify Device Certificates (Step 2 of 3).
7. Click **Device Certificate Matches**.
   The screen shows Add Device (Step 3 of 3).
8. In the **Name** field, type the name of the device you are adding.
9. Click **Add Device**.
   At the upper right, next to the F5 logo, the status of your device should show `ONLINE (ACTIVE)` and `Connected`, with a green indicator next to them showing its active and connected status.

Creating a sync-failover device group

For an HA configuration, you need to establish failover capability between two or more BIG-IP® devices. Then, if an active device in a sync-failover device group becomes unavailable, the configuration objects fail over to another member of the device group, and traffic processing is unaffected. You perform this task on any one of the authority devices within the local trust domain.

1. On the Main tab, click **Device Management** > **Device Groups**.
   The Device Group List screen opens.
2. Click **Create**.
   The New Device Group screen opens.
3. In the General Properties area, name your new device group and select the group type.
   a) In the **Name** field, type the name of your device group.
   b) From the **Group Type** list, select **Sync-Failover**.
4. For the **Configuration** setting, retain the **Basic** configuration type, and then select members and define the sync type.
   a) In the **Members** setting, select available devices from the **Available** list and add them to the **Includes** list.
   b) From the **Sync Type** list, select **Manual with Incremental Sync**.

   Note: *You must do a manual sync. If you select* ***Automatic with Incremental Sync****, your HA deployment will fail.*
5. Click **Finished**.

The Device Groups list screen opens, listing your new device group. The ConfigSync Status column will indicate `waiting Initial Sync`.

Synchronizing the device group

For an HA configuration, you need to synchronize the BIG-IP® configuration data from the local device to the devices in the device group. This synchronization ensures that devices in the device group operate properly. When synchronizing self IP addresses, the BIG-IP system synchronizes floating self IP addresses only.

1. Next to the F5 logo, click **Awaiting Initial Sync**.

   On the Main tab, you can also click **Device Management** > **Overview**.

   The Device Management Overview screen opens, showing your Device Groups.
2. In the Sync Issues area, select **ha** to expand the Devices and Sync Options areas of the screen.
3. In the Devices area, select the device showing `Changes Pending`.
4. In the Sync Options area, select **Push the selected device configuration to the group**.
5. Click **Sync**.

You have now completed your F5® Herculon™ SSL Orchestrator™ HA deployment. Next, set up a basic configuration for deployment on your active device.

Setting up a basic configuration for deployment

You must create identical information on each device before deploying the configuration.

You can now setup a basic configuration for deployment on your active device.

1. On the Main tab, click **SSL Orchestrator** > **Configuration**.
   The General Properties screen opens.
2. Refer to the *Configuring general properties* section for complete instructions.
   After you deploy your configuration on the active device, the system automatically synchronizes the configuration with all of the other devices in the device group. Since some errors may not be apparent, it is critical that you thoroughly test and diagnose the success or failure of the deployment. Refer to *Task summary for diagnosing and fixing high availability deployment* for steps to test and verify your HA deployment.

Task summary for diagnosing and fixing high availability deployment

Before using the methods available in this section, first refer to the *Diagnosing your Herculon SSL Orchestrator deployment* section for detailed information on how to monitor the success or failure of your configuration deployment.

For additional methods that help diagnose, verify, and fix a failed HA deployment, use the following tasks:

- *Verifying deployment and viewing logs*
- *Verifying the RPM file version on both devices*
- *Configuring general properties and redeploying*
- *Reviewing error logs and performing recovery steps*

Verifying deployment and viewing logs

You can verify your deployment by verifying that the required virtuals, profiles, and BIG-IP® LTM® and network objects have been created, checking that the RPM files are in sync, and reviewing logs for failures, for example.

Note: *Because the initial device in the HA device group repeats the configuration requests and propagates the configuration to other BIG-IP devices, make sure you verify the initial configured device first, followed by each device in the HA device group. If the initial device deployment configuration fails, all other device configuration deployments will not successfully be configured.*

---

1. Verify that all expected and required virtuals, profiles, and BIG-IP LTM and network objects (route-domains, VLANs, self IPs) have been created on each device in the HA device group.

   These will be items beginning with the name given to the application (for example, if the application was named SSLO, verify that all of the items named | Summary SSL Orchestrator 13.0.0 | 9 SSLO_* are the same on all devices).
2. Ensure that all RPM file versions are identical.
3. Verify your deployment with, or without, services.
4. Review the following logs for failures:
   - `/var/log/restnoded/restnoded.log`
   - `/var/log/restjavad.0.log`

Verifying the RPM file version on both devices

After a successful F5® Herculon™ SSL Orchestrator™ HA deployment, verify that the latest version of the Herculon SSL Orchestrator zip file is installed on both devices.

1. On the Main tab, click **SSL Orchestrator** > **Updates**.
   The Updates screen opens.
2. Check the RPM versions in the **Version** field.

If the versions are not identical, you must install an updated RPM file and verify that both devices are identically configured.

Configuring general properties and redeploying

If your configured deployment continues to fail, you can remove and reconfigure all general property settings, or restore a previously successful backup file per device.

1. Remove all configurations present on all devices.

   Note: *You may want to restore a backup file instead, per device, to remove all current configurations.*

2. For all devices, individually configure each section in the F5® Herculon™ SSL Orchestrator™ configuration utility and select **Deploy**. Verify that all new objects are properly synced and deployed.

   Note: *If synchronization or deployment issues persist after deploying after each section, attempt to deploy after updating each item (instead of after each section) in the Herculon SSL Orchestrator configuration utility and verify that all new objects are properly synced and deployed.*

   Note: *See the Configuring general properties section for more detailed information.*

Reviewing error logs and performing recovery steps

You can review log messages to help you debug system activity and perform recovery steps. Refer to the *Configuring logging* section of this document for more information on generating logs and setting the level of logging you want the system to perform.

1. Verify that all BIG-IP® LTM®and network objects are present on each of the devices in the HA device group.
2. If the configuration deployment fails on each device, review the logs:
   - `/var/log/restnoded/restnoded.log`
   - `/var/log/restjavad.0.log`
3. Use the following REST GET command to determine the state of the deployed device block in the REST storage:
   - `curl -s -k -u admin:admin` https://localhost/mgmt/shared/iapp/blocks `| json-format`
4. Since failure scenarios can vary, after reviewing the logs, attempt the following recovery steps:
   a) Redeploy Herculon SSL Orchestrator.
      If this succeeds, you have recovered from the failure situation.
   b) Undeploy Herculon SSL Orchestrator.
      By undeploying, a cleanup of MCP objects on each of the devices occurs while also cleaning up required data properties within the block stored in REST storage. If this succeeds, attempt to redeploy again.

c) If redeploy or undeploy fails, do the following:

1. From command line (back door), `run > touch /var/config/rest/iapps/enable`.
2. Refresh the Herculon SSL Orchestrator menu UI.
3. Select the deployed application from the list and delete the application.
4. Redeploy and undeploy again.
5. Once done, remove the file `rm -f /var/config/rest/iapps/enable`.

d) If these recovery steps do not work, you may need to clean up the REST storage.

Note: *For more detailed information on setting up HA, see the BIG-IP Device Service Clustering: Administration document.*

Using Herculon SSL Orchestrator Analytics

Overview: About Herculon SSL Orchestrator analytics

Herculon SSL Orchestrator analytics provide a customizable view into your Herculon SSL Orchestrator statistics, and enable you to flexibly choose the information you want to view based on specified ranges of time that you can select and easily adjust. By leveraging the multiple options available, you can analyze dimensions individually, compare groups of dimensions and their statistics, and sort the charts and tables as you diagnose the performance and health of your system's SSL orchestration.

When you initially launch the analytics dashboard by clicking **SSL Orchestrator > Analytics > Statistics**, data that has been collected over the last hour is displayed in five line charts:

- Hit Count
- Client Bytes In
- Server Bytes In
- Client Bytes Out
- Server Bytes Out

This initial display of data is unfiltered and includes statistics generated for the following dimensions in tables:

- Client Cipher Names
- Client Cipher Versions
- Server Cipher Names
- Server Cipher Versions
- Virtual Servers
- Servers (the final destination)
- Actions

You can also use the Herculon SSL Orchestrator analytics Scheduled Reports to set up an automatic reporting schedule and later view any stored scheduled statistical records.

About analytics dashboard capabilities

The F5® Herculon™ SSL Orchestrator™ analytics dashboard has customizable options so that you can view statistics for your orchestration's top virtual servers, top sites bypassed, top sites decrypted, the most used client ciphers and protocols, and determine where the top server ciphers and protocols are used.

By customizing the timeline, charts, and tables, you can also:

- Adjust the timeline for the statistics displayed in the charts and tables to customize statics captured across a wide range of time, spanning between just a minute up to an entire year.
- Create comparison charts for two or more members of a dimension.
- Filter data across one or more dimensions.
- Sort table-based statistics for any dimension.

Timeline capabilities

The customizable timeline capabilities give you the ability to produce a statistical analysis based on a specified range of time. When you first open the analytics dashboard, the default refresh time is set at 5 minutes. You can change the refresh rate to several different settings by selecting from the **5 min.** list at the top of the screen.

- **1 min.**, **5 min.**, or **10 min.** options reset the refresh time in minutes.
- **Off** freezes the data refresh collection.

You can also update the statistics on demand by selecting **Refresh** above the timeline.

Customizing timeline capabilities

You can customize the range of time in which you would like to view data, in both the charts and tables. When you first launch the analytics dashboard, the default range of time is set at the **Last hour**. You can change the range of time that appears on the timeline to several different settings.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Statistics** to view the default charts, on the left, and dimensions, such as Client Cipher Names, Virtual Servers, and Actions, on the right. The default time for collecting data is set to show statistics gathered over the last hour.
   The Statistics screen opens.
2. Above the timeline, from the **Last hour** list, select the range of time you would like to view statistics across.
   - **Last hour**
   - **Last 4 hours**
   - **Last day**
   - **Last week**
   - **Last month**
   - **Last year**
   - **Year to date**
   - **All**

   The range of time you specified appears above the timeline bar.
3. Use the timeline sliders at each end of the timeline, to manually scroll back and forth, further narrowing in on ranges of time that are critical to the ongoing performance and health of your system's SSL orchestration.

   Once the sliders have been manipulated, you can also click and drag the bar above the timeline based on the newly specified timeline.

Chart capabilities

You can reorder the customizable line charts by dragging them up or down to a different place in the chart stack. You can also minimize them so to hide their information.

Customizing chart capabilities

Within each line chart, you can identify a specific day and time within the time range selected. You can also select a block of time to be further analyzed. By leveraging the multiple options available, you can analyze dimensions individually, compare groups of dimensions and their statistics, and sort the charts as you diagnose the performance and health of your system's SSL orchestration.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Statistics** to view the default charts, on the left, and dimensions, such as Client Cipher Names, Virtual Servers, and Actions, on the right. The default time for collecting data is set to show statistics gathered over the last hour.
   The Statistics screen opens.
2. On the title bar of the line chart, place your cursor anywhere, click and hold to drag the chart up or down the chart stack.
3. On the right side of the title bar, select the minus sign (**-**) to minimize the chart.
4. Select the plus sign (+) to again maximize the chart.

Table capabilities

The customizable dimension tables can be reordered and expanded and minimized just like the line charts. By using the menu at the top of the table on the dashboard, you can expand the tables toward the center of the dashboard so that you can view all the table columns collecting statistics.

Customizing table capabilities

You can select each column within a table individually, and sort it to view the data in ascending or descending order.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Statistics** to view the default charts, on the left, and dimensions, such as Client Cipher Names, Virtual Servers, and Actions, on the right. The default time for collecting data is set to show statistics gathered over the last hour.
   The Statistics screen opens.
2. On the title bar of the table, place your cursor at the beginning of the table's title and click the three lines.
3. Select **Sort By**.
4. Choose one of the table columns to highlight:
   - Hit Count Per Second
   - Client Bytes Out Per Second
   - Duration
   - Server Bytes In
   - Server Bytes In Per Second
   - Hit Count
   - Server Bytes Out Per Second
   - Client Bytes In
   - Client Bytes In Per Second
   - Client Bytes Out
   - Server Bytes Out

You can also individually select each row within a table to update the statistics within each available chart. You can also launch a comparison chart based on the table and the column of data that you selected to sort by.

5. To highlight a table member, within the table, select that row.
6. Right-click the highlighted row and select **Sort By**.
7. Choose one of the table columns you would like to create a chart from, and right-click the highlighted row.
8. Select **Add Comparison Chart**.
   A comparison chart opens displaying the dimension, row member, and statistical column that you chose.

Note: *You can add more comparison charts as needed, reorder new charts added to the chart stack, and minimize them as necessary.*

---

9. To remove the comparison chart, click the **X** in the far-right corner of the chart's title bar.
10. To reset the table without any member of the table highlighted, right-click the highlighted row within the table and select **Clear Selection**.

Charting bytes in, bytes out, and hit count over time

You can use F5® Herculon™ SSL Orchestrator™ statistics to view and analyze bytes in and bytes out for your clients and servers, as well as view the hit count over a determined range of time.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Statistics** to view the default charts, on the left, and dimensions, such as Client Cipher Names, Virtual Servers, and Actions, on the right. The default time for collecting data is set to show statistics gathered over the last hour.

   The Statistics screen opens.
2. To decrease the time range that is being analyzed, adjust the sliders on the timeline at the top of the screen.
   The data found in the charts and tables will adjust based on the new time range specified.
3. To increase the time range that is being analyzed, click **Last Hour** list and select a time range from the list.
4. To focus on specific members of a dimension, click the name of a dimension, on the right, to expand its details and select the members that interest you.
   For example, you might click **Servers** and select one or more servers from the table that displays.

Comparing statistics on the top virtual servers

You can use F5® Herculon™ SSL Orchestrator™ statistics to compare hit count, duration, and hit count per second information across your virtual servers in customized charts that graphically display the results.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Statistics** to view the default charts, on the left, and dimensions, such as Client Cipher Names, Virtual Servers, and Actions, on the right. The default time for collecting data is set to show statistics gathered over the last hour.
   The Statistics screen opens.
2. On the right, expand the **Virtual Servers** dimension.
   By default, the virtual servers are sorted with the busiest at the top.
3. Select two or more virtual servers, then right-click and select **Add Comparison Chart**.
   A new chart displays above the default charts. By default, **Hit Count** is charted for the selected virtual servers.

4. To compare another statistic, in the chart legend click **Hit Count** and select a statistic.
   For example, select **Duration** or **Hit Count Per Second**.
   A line graph displays for the statistic you selected. The comparison chart remains available on your screen as long as you keep your browser open.
5. To remove the comparison chart from the screen, click the **X** in the upper right corner of the chart.

Viewing the top sites bypassed

You can use F5® Herculon™ SSL Orchestrator™ statistics to view and analyze which servers bypass the most SSL requests and perform no decryption.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Statistics** to view the default charts, on the left, and dimensions, such as Client Cipher Names, Virtual Servers, and Actions, on the right. The default time for collecting data is set to show statistics gathered over the last hour.
   The Statistics screen opens.
2. On the right, expand the **Actions** and **Servers** dimensions.
   Data for the dimensions display in tables. By default, those with the greatest hit count display at the top.
3. Rearrange the screen to display more columns of data in the tables:
   - To switch to a table-only view, click the icon.
   - To change the widths of the tables and the charts across the display, drag and drop the icon.
4. In **Actions**, select **Bypassed**.
5. In **Servers**, the servers on which SSL bypass has occurred the most frequently are at the top of the list.

Viewing the top sites decrypted

You can use F5® Herculon™ SSL Orchestrator™ statistics to view and anaylze which servers decrypted the most SSL requests.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Statistics** to view the default charts, on the left, and dimensions, such as Client Cipher Names, Virtual Servers, and Actions, on the right. The default time for collecting data is set to show statistics gathered over the last hour.
   The Statistics screen opens.
2. On the right, expand the **Actions** and **Servers** dimensions.
   Data for the dimensions display in tables. By default, those with the greatest hit count display at the top.
3. Rearrange the screen to display more columns of date in the tables:
   - To switch to a table-only view, click the icon.
   - To change the widths of the tables and the charts across the display, drag and drop the icon as necessary.
4. In **Actions**, select **Intercepted**.
5. In **Servers**, the servers on which decryption has occurred the most frequently are at the top of the table.

Viewing the most used client ciphers and protocols

You can use F5® Herculon™ SSL Orchestrator™ statistics to view and analyze which client ciphers and protocols are used the most. The customizable charts, which graphically display the results, enable you to flexibly choose the information you want to view based on specified ranges of time that you select and can easily adjust.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Statistics** to view the default charts, on the left, and dimensions, such as Client Cipher Names, Virtual Servers, and Actions, on the right. The default time for collecting data is set to show statistics gathered over the last hour.
   The Statistics screen opens.
2. On the right, expand **Client Cipher Names** and **Client Cipher Versions**.
   Data for the dimensions display in tables. By default, those with the greatest hit count display at the top.
3. To view data for the top cipher, from **Client Cipher Names**, select the top record.
   Charts update to display data for the selected cipher only. **Client Cipher Versions** displays only the protocols used by the selected cipher.
4. To view data for the top ten ciphers, from **Client Cipher Names** select the top ten records.

Finding where the top server ciphers and protocols are used

You can use F5® Herculon™ SSL Orchestrator™ statistics to view and analyze which server ciphers and protocols are used the most and locate where they are used. The customizable charts, which graphically display the results, enable you to flexibly choose the information you want to view based on specified ranges of time that you select and can easily adjust.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Statistics** to view the default charts, on the left, and dimensions, such as Client Cipher Names, Virtual Servers, and Actions, on the right. The default time for collecting data is set to show statistics gathered over the last hour.
   The Statistics screen opens.
2. On the right, expand the **Server Cipher Names** and **Server Cipher Versions** dimensions.
   Data for the dimensions display in tables. By default, those with the greatest hit count display at the top.
3. To view data for the top cipher, from **Server Cipher Names**, select the top record.
   Charts update to display data for the selected cipher only. **Server Cipher Versions** displays only the protocols used by the selected cipher.
4. To view data for the top ten ciphers, from **Server Cipher Names** select the top ten records.
5. To view the servers and virtual servers involved in the transactions, on the right expand **Servers** and **Virtual Servers**.
   The tables display only the servers and virtual servers where the cipher and protocol were used.

Scheduling reports to be sent

Before you can schedule reports to be sent, you need to configure SMTP on the system, and have the email addresses of the people to whom you want to send the reports.

You can schedule specific Analytics reports to be sent to one of more email addresses periodically. The reports that are available depend on the modules installed on your system, and how the system is configured. In the schedule, you specify the information to include in the report. For example, if you are a network administrator, you could schedule reports about DNS packets. Resource administrators can

send reports so they can track CPU, disk, and memory utilization, and other system statistics. Many other reports are available that you can schedule to be sent regularly.

Select the information to include in the report.

1. On the Main tab, click **SSL Orchestrator** > **Analytics** > **Scheduled Reports**.
   The Scheduled Reports screen opens.

   Note: *If SMTP is not configured, you receive a message with a link. Click the link to set up SMTP before proceeding.*

2. On the far right, click **Create**.
   The New Reporting Schedule screen opens.
3. In the **Name** field, type a name for the report schedule.
4. In the **Send To (E-Mails)** setting, type an email address where you want to send the report, and click **Add**.
   Add as many email addresses as you need to.
5. From the **SMTP Configuration** list, select the configuration that you want to use.
   If no configurations are available, click **Create** to add one.
6. From the **Reporting Module** list, select the type of report you want to send.

   The types of reports listed depend on which modules you have provisioned on your system.
7. In the **Chart** setting, specify what you want to include in the report. Criteria and measures that you can specify vary for the different types of reports.
   a) In the **Filter** setting, from the lists, select the time period and number of results to show.
   b) In the **Chart Path**, select the top reporting criteria, then select the measures to include in the report.

      The criteria and measures differ depending on which **Reporting Module** you select.
   c) From the **Available measures**, select the ones to include in the report and move them to **Selected measures**.
   d) To drill down and include more specific report criteria, click +, then from the **Use top result** list, select another option.
   e) To include an average of all the statistics and the specific ones, select the **Include Overall** check box below the measures.
8. For **Mail Frequency**, select how often, the date to start, and the time to send the reports.
9. Click **Finished**.

The report schedule is added to the list. The specified report is sent by email to the addresses as scheduled. Or, select the schedule and click **Send Now** to test sending it right away. The report is attached to the email as a PDF. You can check the status in the list to see if the report was sent successfully.

Legal Notices

Legal notices

Publication Date

This document was published on November 20, 2017.

Publication Number

MAN-0645-02

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Link Controller Availability

This product is not currently available in the U.S.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a

residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Index

A

analytics
    about Herculon SSL Orchestrator *47*
analytics charts
    about *48*
    customizing *49*
analytics scheduled reports
    about *52*
analytics tables
    about *49*
    customizing *49*
analytics timeline
    about *48*
application status
    deployed *12*
    error *12*

B

basic configuration
    about *13*
bytes in
    charting *50*
bytes out
    charting *50*

C

charts
    customizing in analytics *49*
    in analytics *48*
classifier rules
    about *27*
configurations
    exporting *36*
    importing new *35*
    importing past *36*

D

dashboard
    for analytics *47*
    for Herculon SSL Orchestrator *47*
    for statistical analysis *47*
dashboard capabilities
    for analytics *47*
deployment
    exporting configurations *36*
    importing new configurations *35*
    importing past configurations *36*
    setting up a basic configuration for *44*
deployment errors
    diagnosing *12*
    viewing details *12*
device group
    creating for sync-failover *43*
device group *(continued)*
    synchronizing *43*
device trust
    implementing *42*
diagnostics *12*

E

egress device
    configuring *16*, *20*
    configuring on system with ingress device *16*
    on one system *16*
error logs
    high availability *45*
explicit proxies
    configuring *24*
explicit proxy
    configuring *23*
exporting
    configurations for deployment *35*
exporting configurations
    about *35*

G

general properties
    configuring *13*

H

Herculon SSL Orchestrator
    deleting *11*
    modifying *11*
    overview *5*
    overview of configuring *9*
    using for initial setup *9*
high availability
    about *39*
    and deployment verification *44*
    and device management *42*
    and device trust *42*
    and local trust domain *42*
    configuration utility version *39*
    configuring ConfigSync *42*
    configuring failover IP address *42*
    creating a device group *43*
    creating sync-failover *43*
    doing manual sync *43*
    fixing deployment *44*
    for deployment *44*
    overview *39*
    prerequisites *40*
    recovery steps *45*
    redeploying *45*
    RPM file version *45*
    self IPs *41*
    setting up a basic configuration *44*

high availability *(continued)*
synchronizing the device group *43*
task summary for deploying *40*
viewing logs for failures *44*
VLANs *41*
hit count over time
charting *50*

I

ICAP services
creating *29*
importing
new configurations for deployment *35*
past configurations for deployment *35*
importing configurations
about *35*
ingress device
configuring *16*, *18*
configuring on system with egress device *16*
on one system *16*
initial setup
of SSL Orchestrator *9*
inline services
creating *27*

L

local trust domain
adding a device *42*
logging
configuring *15*

M

most used client ciphers
viewing *52*
most used client protocols
viewing *52*

R

receive-only services
configuring *30*
RPM file
installing update *41*
rules
creating for TCP *31*

S

scheduled reports
in analytics *52*
server ciphers used
finding *52*
server protocols used
finding *52*
service chain classifier
creating *33*
creating for TCP *31*
creating rules *31*
service chain classifier *(continued)*
rule *33*
UDP *33*
service chains
about *27*
configuring *30*
services
about *27*
sites bypassed
viewing *51*
sites decrypted
viewing *51*
SSL Orchestrator
overview *5*
sync-failover
creating a device group *43*
system configuration
overview *9*

T

tables
customizing in analytics *49*
in analytics *49*
timeline capabilities
about *48*
customizing *48*
timeline sliders *48*
transparent and explicit proxies
configuring *24*
transparent proxy
configuring *23*

U

updated RPM file
installing *41*

V

virtual servers statistics
comparing *50*