7. Select the radio button that determines the format of your SSL keys, then configure their details. Supported formats include:
   - **PEM**: Navigate to the locations of both the public and private keys.
   - **PKCS12**: Navigate to the location of the PKCS12 file, then type the password used to protect the file.
8. Click **Upload**. The relevant key files are uploaded to the SecureSphere gateway.
9. Click **Save**. Settings are saved. If you are in delayed activation mode, you need to activate these settings. For more information, see Activating Settings on page 78.

SSL Ciphers

SecureSphere supports a number of ciphers to enable the decryption and inspection encrypted packets in your network. The following table lists the ciphers supported by SecureSphere and if they are enabled by default. For the ciphers not enabled by default, contact Imperva support for assistance in enabling.

Supported SSL Ciphers

Supported Protocol	SSL Cipher	Enabled By Default
SSLv3	SSL_NULL_WITH_NULL_NULL	No
	SSL_RSA_WITH_NULL_MD5	No
	SSL_RSA_WITH_NULL_SHA	No
	SSL_RSA_WITH_RC4_128_MD5	No
	SSL_RSA_WITH_RC4_128_SHA	No
	SSL_RSA_WITH_DES_CBC_SHA	No
	SSL_RSA_WITH_3DES_EDE_CBC_SHA	No
	SSL_RSA_EXPORT_WITH_RC4_40_MD5	No
	SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	No

Supported TLS Ciphers

Supported Protocol	SSL Cipher	Enabled By Default
TLS 1.0 -1.2	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Yes For NGRP gateways only
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Yes For NGRP gateways only
	TLS_RSA_WITH_IDEA_CBC_SHA	Yes For NGRP gateways only
	TLS_RSA_WITH_SEED_CBC_SHA	Yes For NGRP gateways only
	TLS_RSA_WITH_NULL_SHA256	No

Supported Protocol	SSL Cipher	Enabled By Default
	TLS_RSA_WITH_AES_128_CBC_SHA	Yes
	TLS_RSA_WITH_AES_256_CBC_SHA	Yes
	TLS_RSA_EXPORT1024_WITH_RC4_56_MD5	No
	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	No
	TLS_RSA_WITH_RC4_128_MD5	No
	TLS_RSA_WITH_RC4_128_SHA	No
	TLS_RSA_WITH_DES_CBC_SHA	No
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	Yes
	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	No
TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA256	Yes
	TLS_RSA_WITH_AES_256_CBC_SHA256	Yes
	TLS_RSA_WITH_AES_256_GCM_SHA384	Yes
	TLS_RSA_WITH_AES_128_GCM_SHA256	Yes

Supported SSL Ciphers - Diffie-Hellman

Supported Protocol	SSL Cipher	Enabled By Default
SSLv3	SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	No
	SSL_DHE_RSA_WITH_DES_CBC_SHA	No
	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	No

Supported TLS Ciphers - Diffie-Hellman

Supported Protocol	SSL Cipher	Enabled By Default
TLS 1.0 -1.2	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_DSS_WITH_AES_128_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_DSS_WITH_AES_256_CBC_SHA	Yes For NGRP gateways only

Supported Protocol	SSL Cipher	Enabled By Default
	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_DSS_WITH_SEED_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_AES_128_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_AES_256_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_SEED_CBC_SHA	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_SEED_CBC_SHA	Yes For NGRP gateways only

Supported Protocol	SSL Cipher	Enabled By Default
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Yes
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Yes
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Yes
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Yes For NGRP gateways only
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Yes For NGRP gateways only
	TLS_DHE_RSA_WITH_SEED_CBC_SHA	Yes For NGRP gateways only
	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	Yes For NGRP gateways only
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Yes For NGRP gateways only
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Yes For NGRP gateways only
	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	Yes For NGRP gateways only
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	Yes For NGRP gateways only
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	Yes For NGRP gateways only
	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Yes For NGRP gateways only
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Yes For NGRP gateways only

Supported Protocol	SSL Cipher	Enabled By Default
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Yes For NGRP gateways only
	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Yes For NGRP gateways only
TLS 1.2	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	Yes For NGRP gateways only
	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	Yes For NGRP gateways only
	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	Yes For NGRP gateways only
	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	Yes For NGRP gateways only
	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	Yes For NGRP gateways only
	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	Yes For NGRP gateways only
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Yes
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Yes
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Yes
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Yes

Supported Protocol	SSL Cipher	Enabled By Default
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Yes
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Yes
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Yes
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	Yes For NGRP gateways only
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	Yes For NGRP gateways only
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	Yes For NGRP gateways only
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	Yes For NGRP gateways only
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	Yes For NGRP gateways only
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	Yes For NGRP gateways only
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	Yes For NGRP gateways only
	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	Yes For NGRP gateways only
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Yes For NGRP gateways only
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Yes For NGRP gateways only
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Yes For NGRP gateways only
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Yes For NGRP gateways only
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Yes For NGRP gateways only
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Yes For NGRP gateways only

Note: For both SSL and TLS, the Diffie-Hellman (DHE) ciphers are:

- Supported only in Kernel Reverse Proxy, Transparent Reverse Proxy and NGRP modes, not in Bridge or Sniffing modes.
- By default, KRP and TRP modes are configured for 1024 bit encryption, but can be configured for 512 bit encryption. For more information on how to change the key size, refer to the Imperva Customer Portal Knowledge Base article: "How To change Diffie Hellman key size from 1024 bit to 512 bit".
- By default, NGRP mode is configured for 2048 bit encryption, but can be configured for 1024, 3072 and 4096 bit encryption. For more information on how to change the key size, contact Imperva support.

Adding Session Identifiers Used for Session Tracking

Session identifiers are pieces of data used to identify a session. SecureSphere uses session identifiers as an alternative to IP addresses to identify users when monitoring and blocking traffic. They are also used to track session related violations such as read only parameter, cookie protection, web data base correlation, and more. It is important the SecureSphere have the correct sessions to ensure that operations is properly conducted such as profiling of session related elements.

SecureSphere is automatically installed with a list of standard session identifiers for most major applications. However, your network or applications may use custom identifiers. In order to get SecureSphere to properly identify all relevant traffic, you need to add these identifiers. Session identifiers are a global object. For instructions on how to configure the Session Identifiers global object, see Configuring Session Tracking on page 327.

Configuring Action Sets and Followed Actions

As part of basic SecureSphere configuration, you may want to configure certain policies to send alerts by e-mail or to a third party event management system such as Arcsight or Remedy. You can configure an action set to meet your needs, then attach it as a followed action to the required SecureSphere object. For instructions on how to configure Action Sets and Followed Actions, see Working with Action Sets and Followed Actions on page 360.

Activating Settings

The need to activate a setting once it has been configured depends on the current activation mode. SecureSphere has two activation modes:

- **Immediate Activation mode (Default)**: Immediately saves and updates the configuration on the server and sends it to the connected gateways.
- **Delayed Activation mode**: Enables you to make a number of changes to the configuration, then activate them at once. This provides better control over changes and helps to minimize mistakes. When in delayed activation mode, changes made in the following locations require activation after saving:
  Main > **Setup**
  Main > **Policies**
  Admin > **ADC**

Note: Depending on the number of changes that have been made, activation may take an extended period of time. The more items that need to be activated, the longer activation takes.