# Options for secure communications

The various options for secure communications between the following components is discussed below:

- NightWatchman Management Center Console
- NightWatchman Management Center Console service
- NightWatchman Management Center Web service
- NightWatchman Management Center Report Console (Web reports)
- WakeUp Console
- WakeUp server
- Web WakeUp
- Enterprise View
- 1E NightWatchman Agent
- Tachyon Agent with the WakeUp module enabled

A summary of how communications are encrypted and secured is as follows:

1. If HTTPS, it must be used by all components, with the exception of the WakeUp server which can use only HTTP to communicate with the NightWatchman Web service.
2. WakeUp server supports only HTTP when it registers with and queries the NightWatchman Web service.
3. HTTP/S is used by the NightWatchman and WakeUp Agents to report data to the NightWatchman Web service, which is encrypted by default using RC2, but can be optionally configured to use AES256 (FIPS) instead by enabling the `USEFIPS` setting. By default, the Web service uses anonymous authentication. NTFS permissions can be used to control access if clients are in trusted domains and Windows Authentication is enabled.
4. HTTP/S is used by policy queries and policy downloads, as used by the agent components for WakeUp alarm clocks and NightWatchman, which are unencrypted (does not use RC2 or AES256 FIPS). By default, the Web service uses anonymous authentication. NTFS permissions can be used to control access.
5. HTTP/S is used by NightWatchman Web reports and Web WakeUp and Enterprise View Web sites, which are unencrypted (does not use RC2 or AES256 FIPS). By default, the websites use Windows authentication. NTFS permissions can be used to control access to each web site.
6. HTTPS uses SSL/TLS and requires a server (SSL) certificate.
7. Websites using SSL/TLS can be configured to require a client authentication certificate, which requires a matching server certificate.
8. If FIPS compliance feature is used (introduced in v6.0.500), then it must be used by all components.
9. RC2 encryption is not FIPS compliant.
10. AES256 encryption is FIPS compliant. This uses the advanced encryption standard algorithm with symmetric key encryption and block size 256.
11. Proprietary communications is used between WakeUp agents and WakeUp server which supports encryption, using the `ENCRYPTIONLEVEL` or `USEFIPS` settings. By default, `EncryptionLevel` is disabled (0), but can be configured to use either `full encryption` (2) which uses RC2 or `FIPS` (3) which uses AES256.
12. `ENCRYPTIONLEVEL` 1 is a hybrid of 0 and 2, and is permitted only on WakeUp servers during gradual transition of clients from `none` (0) to `full` (2) and is never used on clients. Gradual transition to `FIPS` (3) is not permitted, and all clients must switch at the same time. FIPS is enabled using the `USEFIPS` setting, which overrides the `ENCRYPTIONLEVEL` setting.
13. Remote NightWatchman Consoles communicate with the NightWatchman Console service using Windows implementation of TLS which is encrypted.
14. Remote WakeUp consoles and the NightWatchman Console service communicate with the WakeUp server service using WMI via DCOM which is not encrypted but secured by Active Directory and firewalls.
15. When WakeUp server is integrated with Configuration Manager, it uses WMI via DCOM to get data from the local or remote SMS Provider role, which is not encrypted but secured by Active Directory and firewalls.
16. The NightWatchman Console Service account, and application pools used by NightWatchman Web reports, Web WakeUp and Enterprise View Web sites use SQL to update and query the NightWatchman database. SQL communications uses default Windows integrated trusted authentication.

## Configuring the NightWatchman Management Center Web service, report console and Web WakeUp

NightWatchman Management Center Web service, report console and Web WakeUp are assumed to be installed under the same Website using the same HTTPS port number (default is 443). Configuration of IIS and certificates are beyond the scope of this discussion.

To configure the Website to use secure communications::

1. Install certificates to the certificate stores on the Web server.
2. Optionally, deploy the client authentication certificate to clients.
3. On the IIS Web server, ensure the default Website uses the default binding for HTTP port 80. Alternatively, disable the default Website and create a new one using HTTP port 80.
4. Install the NightWatchman Management Center Web service (AFWebService) and Report Console components using default settings for IIS ports and host headers.
5. Install Web WakeUp using the default settings for IIS port and host header.
6. After installation, add an HTTPS binding that uses the server (SSL) certificate. The HTTP binding must be kept for the Website used by AFWebService in order to support WakeUp server's HTTP requirement.
7. Deploy the 1E Agent using the `SECUREREPORTINGSERVER` property with optional use of `CERTISSUER` or `CERTSUBJECT` and `ENCRYPTIONLEVEL` or `USEFIPS` properties.

## HTTPS and SSL

HTTPS encrypts communications and uses an SSL certificate issued by an external certification authority (CA) or by a server that acts as a CA on your Windows domain. If HTTPS is used, then it must be used by all components (the NightWatchman Web service, WakeUp server and 1E Agent). The exception is the NightWatchman Report console and Web WakeUp which can use HTTP instead, but it makes sense for all to use HTTPS.

Server components using HTTPS must be installed under the same Website, using an HTTPS binding (including port) that uses the server (SSL) certificate. The SSL certificate must be imported into the Web server before it can be used. You cannot install components with different host headers under the same or separate Websites on one Web server. The ability to use multiple host headers requires a server (SSL) certificate that supports all the names.

If a mixture of HTTPS and HTTP is required, the NightWatchman Report console and Web WakeUp can be installed in on separate Website with an HTTP binding and host header. If a host header is required for HTTPS, the server (SSL) certificate must support this requirement and the CN used in the certificate must match the fully qualified host header.

Configure the 1E Agent to use HTTPS with the `SECUREREPORTINGSERVER` property (see client configuration). The NightWatchman and WakeUp components will use HTTPS for reporting and for policy retrieval.

### Client certificate authentication

In addition to HTTPS and SSL, the SSL configuration of the Web server can optionally be configured to request a client certificate. The client certificate is installed on all clients. The server prompts the client for a valid client authentication certificate for mutual authentication.

The 1E Agent must be configured to use HTTPS as above, and either `CERTISSUER` or `CERTSUBJECT` properties, (see client configuration). The NightWatchman and WakeUp components iterate through their local certificate store to match a certificate by issuer or by subject to send back to the server when challenged. The server validates the CA in the certificate before initiating the connection.

Specific items that must be taken into account when setting up client certificates for authentication are:

| Items for consideration | Description |
|---|---|
| Required certificates | To enable secure channel communications the server requires an SSL certificate. For client authentication, a client authentication certificate is required in each of the client's certificate store and a matching certificate from the same certification authority is required in the server certificate store. |
| Locating certificates on the client certificate store | Certificates must be located either in the Third Party Root Certification Authorities or Trusted Root Certification Authorities stores. |
| Multiple certificates with the same Subject and Issued By fields | We recommend you only define a single certificate for a particular Subject and Issued By fields although you can define multiple certificates with the same Subject and Issued By fields. NightWatchman clients and WakeUp Agents will only return the first certificate found matching the Subject and Issued By fields. |
| Revoking certificates | Trust is based on the CA certificate entries in the Web server's Trusted Root Certification Authorities machine certificate store. When you revoke a certificate, remove them from the server certificate store. |

## Agent configuration

- Using HTTPS and SSL – to use `HTTPS`, specify the `SECUREREPORTINGSERVER` property on the NightWatchman Agent installer command-line. Set it to the fully qualified domain name for the server hosting the NightWatchman Management Center Web service. NightWatchman and WakeUp components to use HTTPS for reporting and for policy retrieval. For example, `msiexec /i 1ENightWatchmanAgent-x64.msi SECUREREPORTINGSERVER="ACMESVR.ACME.COM" /qn`
- Using HTTPS, SSL and client certificate authentication – to use `HTTPS` with client certificate authentication, you will also need to set the `CERTISSUER` or `CERTSUBJECT` properties on the 1E Agent installer command-line to either the name of the certificate issuer or subject respectively. For example, `msiexec /i 1ENightWatchmanAgent-x64.msi SECUREREPORTINGSERVER="ACMESVR.ACME.COM" CERTSUBJECT=ACMECOMS /qn`
- Using ENCRYPTIONLEVEL or FIPS – `ENCRYPTIONLEVEL` determines the level of encryption used for communications between WakeUp agents and WakeUp servers. The same setting must be used on all WakeUp components. The exception is where the configuration of the agent is in the process of being changed between `none` (0) to `full encryption` (2), or vice versa, resulting in a mix of agents being supported by the same WakeUp servers. Set the WakeUp servers to use `partial` (mixed) encryption (1) until all the agents have been updated.

  ```
  msiexec /i 1ENightWatchmanEAgent-x64.msi ENCRYPTIONLEVEL="2" /qn
  msiexec /i WakeUpSvr.msi ENCRYPTIONLEVEL="2" /qn
  ```

  If FIPS compliance is required, use the `USEFIPS` settings instead. FIPS overrides the use of `ENCRYPTIONLEVEL`, therefore only one of these properties is set, not both. When using FIPS, all WakeUp and NightWatchman components must be configured identically, mixed settings are not possible.

  ```
  msiexec /i 1ENightWatchmanAgent-x64.msi USEFIPS="1" /qn
  msiexec /i WakeUpSvr.msi USEFIPS="1" /qn
  Msiexec /i NightWatchmanManagementCenter.msi USEFIPS="TRUE" /qn
  ```

### Summary of installer properties

#### NightWatchman Management Center

- USEFIPS

### WakeUp server

- SECUREREPORTINGSERVER
- CERTISSUER or CERTSUBJECT
- ENCRYPTIONLEVEL or USEFIPS

### Web WakeUp

- None

### 1E NightWatchman Agent

- SECUREREPORTINGSERVER
- CERTISSUER or CERTSUBJECT
- ENCRYPTIONLEVEL or USEFIPS