PureConnect®

2018 R5

Generated:

12-November-2018

Content last updated:

25-January-2018

See Change Log for summary of changes.

GENESYS™

Interaction Supervisor iPad Edition

Administrator's Guide

Abstract

This document provides system administrators with information on SSL certificates and other configuration tasks of Interaction Supervisor iPad Edition.

For the latest version of this document, see the PureConnect Documentation Library at: http://help.genesys.com/cic.

Table of Contents

Interaction Supervisor iPad Edition introduction

Interaction Supervisor iPad Edition is a performance monitoring system for mobile CIC contact center supervisors. It provides contact center statistics about people and queues. This iOS app for iPad is available from the App Store. iPad is a trademark of Apple, Inc.

Executives, supervisors, managers, and IT professionals can us Supervisor iPad Edition to monitor agents and queue activity in real-time. Supervisor provides immediate operational information and notifications for special events.

Important!
To use Interaction Supervisor iPad Edition, an **I3_ACCESS_IPAD_USER_SUPERVISOR** access license must be assigned to the user. This assignment is performed in Interaction Administrator from the Licensing tab of a user properties dialog.

Interaction Supervisor iPad Edition uses **Interaction Center Web Services** (**ICWS**), a scalable web service interface that connects Customer Interaction Center with client applications. ICWS provides the connectivity that a client application needs to work with interactions, directories, people, configuration, and statistics. ICWS manages connections with CIC and performs actions for the connected session user.

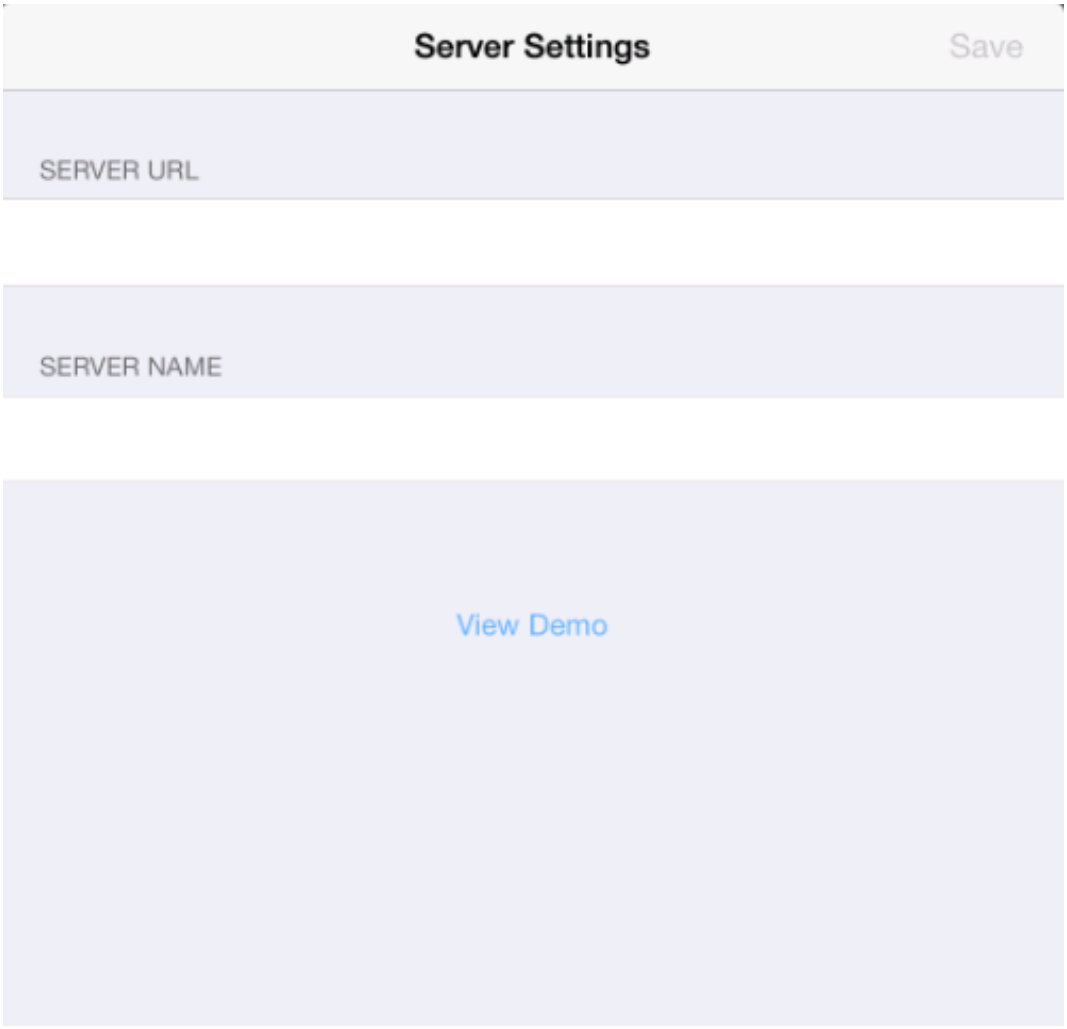
The instructions in this document help system administrators set up ICWS certificates to support users of Interaction Supervisor iPad Edition. For the convenience of the administrator, some of the information in this document is extracted from *CIC Security Features*.

If you need more information about security features in Customer Interaction Center, see *CIC Security Features*. *CIC Security Features* covers use of Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure RTP (SRTP) protocols. It also covers public key cryptography and certificates that enhance application security.

This content contains the following major topics:

Configure server settings

The first time you launch Supervisor iPad Edition, you configure the server settings. You can configure either a direct or a reverse proxy connection to the Interaction Center Session Manager server.



Configure a **direct connection** when you want the iPad to communicate with an Interaction Center Session Manager server directly.

Choose a **reverse proxy** when you want the hostname of the Interaction Center Session Manager server to be located in the path component of the URL.

For more information on reverse proxies, see https://developer.inin.com/documentation/Documents/ICWS/WebHelp/ConceptualContent/Concepts_WebProxies.htm.

About the reverse proxy connection process

This section describes the events that occur when a user attempts to connect by way of a reverse proxy configured as `https://reverse-proxy/internal`.

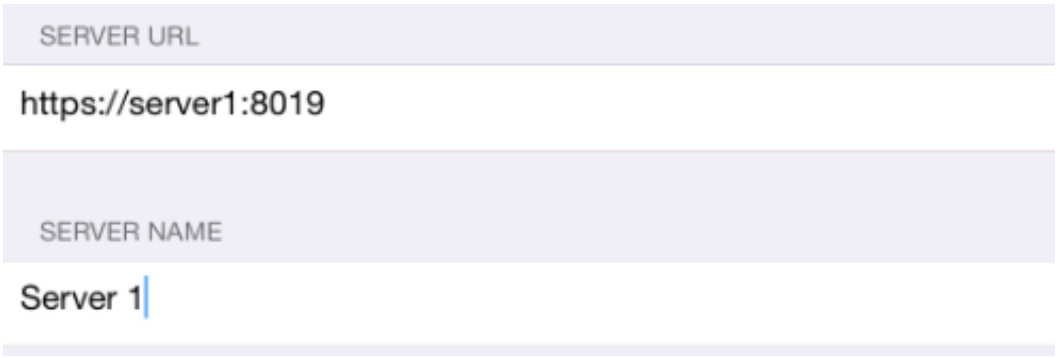
1. A request is made to the following URL address:
   `https://reverse-proxy/internal/config/servers.json`
2. A response is returned with status code `200`, a Content-Type of `application/json`, and the following JavaScript Object Notation (JSON) message body:

```
{
  "version": 1,
  "servers": [
    { "host": "server1.company.local", "displayName": "Server 1" }
  ],
  "serviceUrlTemplate": " https://reverse-proxy/internal/api/{host}/"
}
```

3. A connection attempt is made to the following URL address:
   `https://reverse-proxy/internal/api/`***`server1.company.local`***`/icws/connection`
   `server1.company.local` in the above URL represents the Fully-Qualified Domain Name (FQDN) of the CIC server.
4. After a successful connection is made, subsequent requests for the session will have the following base URL address:
   `https://reverse-proxy/internal/api/`*`server1.company.local/`*

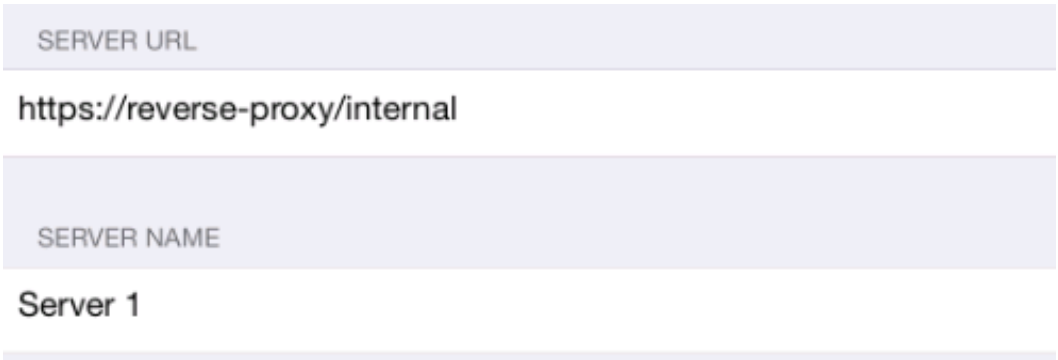
Configure the server connection

1. In the **Server URL** box of the **Server Settings** page, do one of the following actions:
   - To configure a direct connection, enter the URL address of the ICWS endpoint.



> **Note:**
> If you are configuring the product for use in a switchover environment, specify only one of the servers in the **Server URL** box. If you specify the backup server, it will respond with a message pointing to the active server.

   - To configure a reverse proxy connection, enter the base URL address to use for all connections.



> **Note:**
> You must also create a file named `servers.json` at the relative URL address in the path `/config/servers.json`. This file must be accessible by the iPad.
>
> If you are using iPad Supervisor Edition 2.1 or higher and CIC version 2015 R4 or higher, you can use an `althosthints` entry from the `servers.json` file. This entry enables you to specify either a CIC server or an Off-Server Session Manager (OSSM) as the connection entry. For more information, see *CIC Web Applications Guide* in the PureConnect Documentation Library.

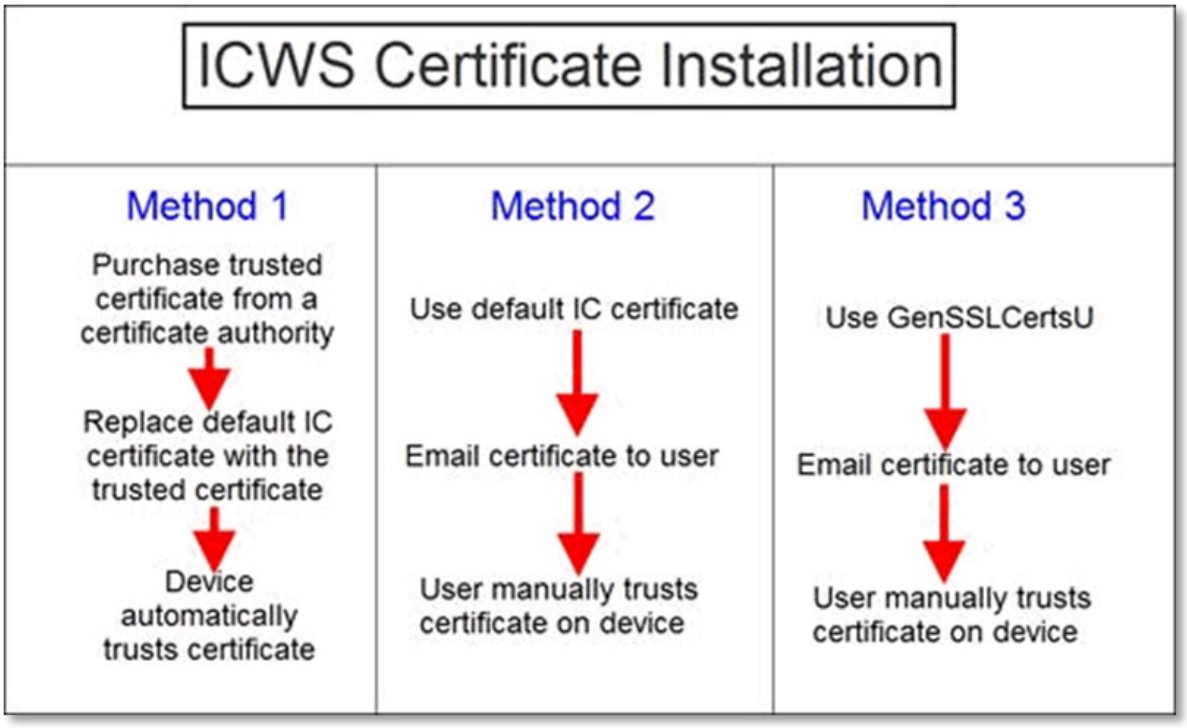
2. In the **Server Name** box, enter a meaningful name for the server.

Web server certificates for iPad apps

IC Web Services (ICWS) supports both secure (HTTPS) and non-secure (HTTP) connections. To secure ICWS connections using SSL, administrators must install certificates on the web server as SSL is enabled in ICWS by default.

Note:
Secure Sockets Layer (SSL) is a protocol for exchanging information privately over the Internet. SSL data is encrypted using a public key known to everyone and a private key known to the recipient only. By convention, URLs that require an SSL connection start with *https* instead of *http*.

Use one of the following three methods to enable security certificates with ICWS:



Method 1

Purchase a security certificate from a trusted authority such as VeriSign, Comodo, or GoDaddy. Because the certificate is from a trusted authority, iPads and other devices automatically trust the certificate.

If you purchase a certificate, place it in one of the following directory paths:

- CIC server:
  `D:\I3\IC\Certificates\HTTPS`
- Off-Site Session Manager server:
  `C:\Program Files (x86)\Interactive Intelligence\Certificates\HTTPS`

Method 2

Use the default security certificate automatically generated during the CIC installation. The default certificate is self-signed, so the user must manually trust the certificate on the iPad or other device.

Method 3

Use the `GenSSLCertsU.exe` utility to generate and install a trusted certificate on the CIC server. You must then manually trust the certificate on the iPad or other device. For more information, see Generating certificates manually with GenSSLCertsU.

Generate and install a trusted certificate for the web server

The web server on the CIC server, such as the one used by the CIC Web Services, requires its own trusted certificate. The separate certificate enables you to control which certificates serve which security purposes.

Use the `GenSSLCertsU.exe` utility with the `-w` parameter to generate the Web Server certificate.

Generating certificates manually with GenSSLCertsU

Setup Assistant and CIC generate most certificates automatically. However, there are situations in which you must generate certificates manually, as shown in the following examples:

- If your organization wants to serve as its own Certificate Authority and sign its own certificates
- If the folder containing your certificates on the CIC server is deleted or corrupted

> **Note:**
> Make backups! Back up your certificates folder, typically in `\I3\IC\Certificates`, so that you have spare copies of all your certificates. However, if you do not have a backup copy of your certificates, you can use the `GenSSLCertsU.exe` utility to regenerate them.

By default, `GenSSLCertsU.exe` is installed in the following directory path:

```
D:\I3\IC\
```

To generate or regenerate certificates, execute `GenSSLCertsU.exe` with the `-w` parameter as displayed in the following example:

```
D:\I3\IC\gensslcertsu -w
```

> **Note:**
> Except for its own optional parameters, you cannot combine `gensslcertsu -w` with other parameters, such as `-r` and `-d`. For more information on all `gensslcertsu.exe` parameters, see "Generating Certificates Manually with GenSSLCertsU" in *Security Features Technical Reference* in the PureConnect Documentation Library.

You can also specify additional parameters after the `-w` parameter as defined in the following table:

Parameter	Description
`-m` *`CNName`*	The `-m` *`CNName`* parameter specifies the common name of the certificate subject. Use the Fully-Qualified Domain Name of the host. Example: `gensslcertsu -w -m server1.example.com`

`-h` *`Path`*	The `-h` *`Path`* parameter specifies the directory path for the certificate and the private key. By default, the certificate and its private kay are stored in the following CIC subdirectory:
	`Certificates\HTTPS`
	For a default installation on the CIC server, the full path is as follows:
	`D:\I3\IC\Certificates\HTTPS`
	Note:
	The path must exist and `gensslcertsu.exe` must have access rights to create and write files to the folder.
	Example:
	`gensslcertsu -w -m server1.example.com -h \Certificates\HTTPS`

`[NotifierHost]` *`[ICUserName`* *`[ICUserPassword]]`*	**Tip:** Square brackets (`[]`) indicate that the optional additions. You can include the brackets in your `gensslcertsu -w` command or not. The *`NotifierHost`* option specifies the CIC server host name, which provide the Notifier communication protocol. Example: `gensslcertsu -w -m server1.example.com MyCICServer`

Parameter	Description
	The *ICUserName* option specifies the name of a CIC user account under which this command has access right to generate certificates. Use this option only if you use the NotifierHost option. **Note:** If you do not specify the *ICUserName* option, gensslcertsu.exe uses the account of the current logged-in user. Example: `gensslcertsu -w -m server1.example.com MyCICServer Admin`
	The *ICUserPassword* option specifies the password of the CIC user account specified with the *ICUserName* option. Use this option only if you use the *ICUserName* option. Example: `gensslcertsu -w -m server1.example.com MyCICServer Admin 1234`
[-a *SHAAlgorithm*]	The -a *SHAAlgorithm* option and parameter specifies that gensslcertsu -w will create certificates using the SHA1 or SHA256 signature digest algorithm. Substitute one of the following items for the SHAAlgorithm parameter: • sha1 • sha256 **Note:** If you do not specify the *SHAAlgorithm* parameter, gensslcertsu.exe uses the SHA1 signature digest algorithm. Example: `gensslcertsu -w -m server1.example.com -a sha256`
[-e]	The -e option specifies gensslcertsu -w to use existing certificates. Use this option with the -a option to use existing certificate information and key pairs when changing the signature digest algorithm. Example: `gensslcertsu.exe -w -m server1.example.com -a sha1 -e`

Email Supervisor iPad Edition users

If you used the default CIC certificate (Method 1) or generated a new certificate using GenSSLCertsU.exe (Method 2), you must email the SSL certificate to all Interaction Supervisor iPad Edition users. You do not need to email a certificate if you purchased it from a certificate authority (Method 3).

To distribute a certificate:

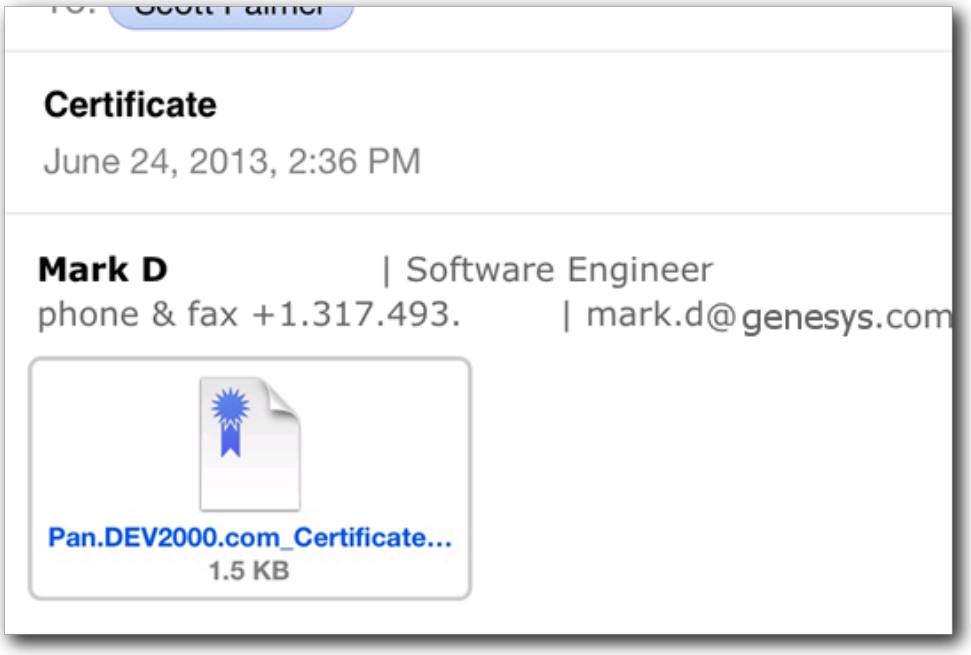
1. Create an email message that provides instructions to the user about how to open the attachment and trust the certificate. For more information, see Install the certificate on the iPad or another device.
2. Attach the certificate to the email message.
3. Send the email to Interaction Supervisor iPad Edition users.

Install the certificate on the iPad or another device

To install the certificate, the administrator must securely deliver the certificate to the user of the iPad or other client device. The user opens the certificate on the device, installing it locally. The CIC app can then use the certificate to connect securely to ICWS on the CIC server.

Complete the following steps to install the certificate on an iPad:

1. From the iPad, open the email message.
2. Tap the icon for the attached certificate.



3. From the **Install Profile** dialog, tap **Install**.

4. If a **Warning** dialog appears, tap **Install**.

5. If prompted, enter the numeric code used to unlock your iPad.
6. When the **Profile Installed** dialog appears, tap **Done**.

Users can now establish a secure connection to the server.

Error messages about trusted certificate

The iPad app does not detect SSL requirements. The iPad does not know if SSL is required by the server until it attempts to connect to session manager. By default, ICWS allows non-SSL connections on port 8018, and SSL connections on port 8019.

The iPad Edition users enter the endpoint address as instructed. For example, users might configure the app to use `http://SM:8018` or `https://SM:8019` where *SM* is the Fully-Qualified Domain Name (FQDN) of a CIC session manager.

- If users specify a port reserved for SSL, such as 8019, and the server does not require an SSL certificate, the connection fails with the following error message:

  The certificate for this server is invalid. You might be connecting to a server that is pretending to be *sessionManagerName* which could put your confidential information at risk
- If the app user does not have a required certificate or has not trusted the certificate, the connection fails with the following error message:

  Receiving an "Invalid server certificate" error when trying to connect to an https endpoint.
- If the endpoint certificate is trusted by a commercial certificate authority, users can connect using the following URL address:

  `http://SM:8019`

  SM represents the FQDN of a CIC session manager.

Configure CIC for images used by the Locator

To use the Locator feature, users do not need to configure the iOS application. However, an administrator must configure the CIC server to store the location where user photos are hosted on a web server.

To support the Locator feature, add the `INTERNAL_USER_PIC_URL` CIC server parameter in Interaction Administrator. The optional parameter specifies a URI with a string replacement (`{0}`) for the user ID of the current user, which points to the corresponding user photo based on the user ID.

Example:

```
http://intranet.example.com/users/{0}.png
```

Specifying `{0}` in the URI string substitutes the currently selected user ID into the URL string. Once the placeholder is processed, the resulting value is fully qualified URI pointing to an image.

Image Sizing Guidelines:

- Photos should be no larger than 128 x 128 pixels. Larger photos are scaled to 128x128 pixels.
- Location images are scaled to fit within the working space of the active monitor.

No security rights are associated with this feature. It is enabled for all users by specifying a valid value for the server parameter. Since the parameter points to an image location, the administrator is responsible for hosting images at each specified URI.

Enable agent queue viewing

From the iPad **Agent Details** modal, supervisors can view a selected agent's user queue if the **User Queue** view right is enabled for that agent.

All interaction types are shown in the user queue, but the supervisor user can only take call control actions on call interactions.

The iPad view shows queue interactions in rows, using interaction attributes which correspond to **queue columns** in other client applications. The queue and interaction detail views are configured by the following **Queue Column Rights**:

- Name
- Number
- Details
- Duration
- State
- Queue
- Interaction Id

The call control buttons do not appear on a supervisor's iPad unless they have the appropriate security rights.

Configure supervisor rights to activate and deactivate agents

From the iPad **Change Activations** modal, supervisors can activate and deactivate agents if granted the following rights:

- **View** rights to the **agent workgroups** so that they appear in the list of queue activations.
- **View** rights to **activated** status or **activate self/others** for at least one member workgroup so that the supervisor can see activation statuses.
- **Activate self/others** is required to enable a supervisor to activate and deactivate agents.

Change log

Date	Changes
29-April-2014	Initial Release
19-September-2014	Updated documentation to reflect changes required in the transition from version 4.0 SU# to CIC 2015 R1, such as updates to product version numbers, system requirements, installation procedures, references to Interactive Intelligence Product Information site URLs, and copyright and trademark information.
04-August-2015	• Updated title page and copyright information. • Added the section, Configure server settings.
04-March-2016	• Updated title page and copyright information. • Updated the notes in the section, Configure the server connection.
21-September-2016	• Updated title page and document abstract. • Updated Copyright and trademark information page. • IOSAPPS-518 - Corrected typographical error in an example for `GenSSLCertsU.exe` command-line utility. • Reformatted and rewrote `GenSSLCertsU.exe` command reference table in Generating certificates manually with GenSSLCertsU. • Made General edits and layout modifications to comply with corporate and departmental standards.
25-January-2018	Conversion to HTML.