Foreseer

Installation and Upgrade Guide

Powering Business Worldwide

Server Installation Guide

Foreseer is designed to manage critical sites and enterprise infrastructures by monitoring power and environmental inputs from equipment, sensors and other systems. Monitored points include Meter (analog) and Status (digital) inputs which open a detailed window into the past, present and future performance of your mission-critical equipment. The unique networked architecture and modular design make Foreseer a cost-effective approach to managing your site while maintaining unique analysis and multi-vendor connectivity capabilities. It furnishes a single integrated system that provides real-time and historical views into the operation of the power and environmental conditions that support your critical operation.

The Foreseer Server functions as a centralized storage location for information from managed Devices and the Foreseer web interface acts as a portal for device and channel configuration, as well as a retrieval and display terminal for that information. Together, the applications allow you to observe real-time data, respond to events and alarms, as well as view historical data and project potential failure for every data input. Your system has been pre-configured during installation with equipment, critical data points and other views specific to your operation.

The configuration can be readily modified to meet your changing monitoring needs.

System Requirements

Please see the Foreseer Release notes document for the most up to date system requirements.

Hardware and Security Considerations

Foreseer also has certain hardware and software prerequisites that must be addressed prior to installing the program on the Server. Hardware prerequisites consist of completing the Configuration Checklist for all of the Devices to be monitored, then establishing physical connections between the Server and the Devices to be monitored.

Security Considerations consist of the following best practices:

- Physical access to server hosting Foreseer and the associated system should be restricted, monitored and logged at all times.
- Physical access to the communication lines should be restricted to reduce the risk of intrusion.
- Attacker with unauthorized physical access to the device could cause serious disruption of the device functionality. A combination of physical access controls to the location should be used, such as locks, card readers, and/or guards etc.
- Access to physical ports and removable media should be controlled and limited.
- Do not connect unauthorized USB device, CD/DVD or SD card for any operation (e.g. Firmware upgrade, Configuration change and Boot application change).
- Before connecting any portable device through USB, CD/DVD or SD card slot, scan the

device for malwares and viruses.
- Foreseer servers should be deployed on systems with limited access to the internet and less trusted networks. The use of email and other functions not necessary for Foreseer to operate should be limited and protected appropriately.

You should restrict access to ports through the Windows Firewall. Foreseer needs the following ports:

- Port 80 (disabled by default in Apache), required only if you allow HTTP access to WebViews and WebAdmin. HTTP access is inherently insecure and is not recommended.
- Port 81, (disabled by default in the Foreseer web server), required for HTTP access for the Legacy Message Manager. HTTP access is inherently insecure and is not recommended.
- Port 443, required for HTTPS access for WebViews, WebAdmin and WebConfig Utility.
- Port 444, required for Remote/Redundant Foreseer Servers and Message Manager.
- Port 2100, required for Remote/Redundant Foreseer Servers.
- SMTP port 25 for Message Manager to be able to send e-mails
- Various ports based on device communication requirements such as Modbus, BACnet and SNMP

SQL Server may require additional ports.

Before proceeding with the installation, it is recommended that you complete the enclosed Configuration Checklist to use as a reference during program installation. Refer to the end of this guide for a copy for a printable copy of the Configuration Checklist.

Security Considerations for Interactive Remote Access

Interactive remote access to Foreseer or third-party communication interfaces should be limited and secured. Windows Remote desktop access should be configured according to the following:

- Only allow log in from specific hosts. You can use whitelist using the Windows Firewall.
- Use client encryption Network Level Authentication (NLA).
- Limit access to users in a designated remote access group; e.g., create a group in Active Directory and assign users or user.
- Limit access to explicit machines; i.e., whitelist access.
- Always prompt for client credentials; i.e., do not store credentials.
- Delete temporary folders when session ends.
- Apply account lockout policy (< 30 minutes default).

SQL Server Installation

SQL Server 2016 Express is shipped with Foreseer and installation is straightforward. SQL Server 2016 Express uses .NET 4.6. The SQL Server Client tools are a required install. They

can be included during the install options within a SQL server installation or found in the Foreseer directory if needed after the install. SQL Server Management Studio is not a requirement but is recommended as a necessary tool for managing SQL Server data and access.

The default configuration of SQL Server 2016 Express enabled Shared Memory access only. Foreseer will connect to SQL Server using TCP/IP connectivity. Upon installing SQL Server 2016 Express, be sure to launch the SQL Server Configuration Manager utility and enable TCP/IP protocol for the SQLEXPRESS named instance.

For a complete step-by-step, please refer to Microsoft documentation at the following link:

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-or-disable-a-server-network-protocol?view=sqlallproducts-allversions

Server Installation

The Foreseer installation and configuration is a three-step process: Program Installation, Server Configuration and Device Configuration. All three steps use a series of wizards to simplify the procedure and user prompts guide you through the entire process.

> If upgrading from a previous version of the Foreseer Server, this procedure should only be performed by experienced personnel through a scheduled site visit.
>
> If upgrading on the same server, it is a simple install over the top of the existing Foreseer installation
>
> If upgrading to a new server, install the Foreseer application on the new server and move the Foreseer 6.3 ARQ from the old Foreseer server and restore to the new Foreseer server.

> Foreseer should be installed on the local hard drive with the most available disk space. In some cases, this may not be the C: drive.

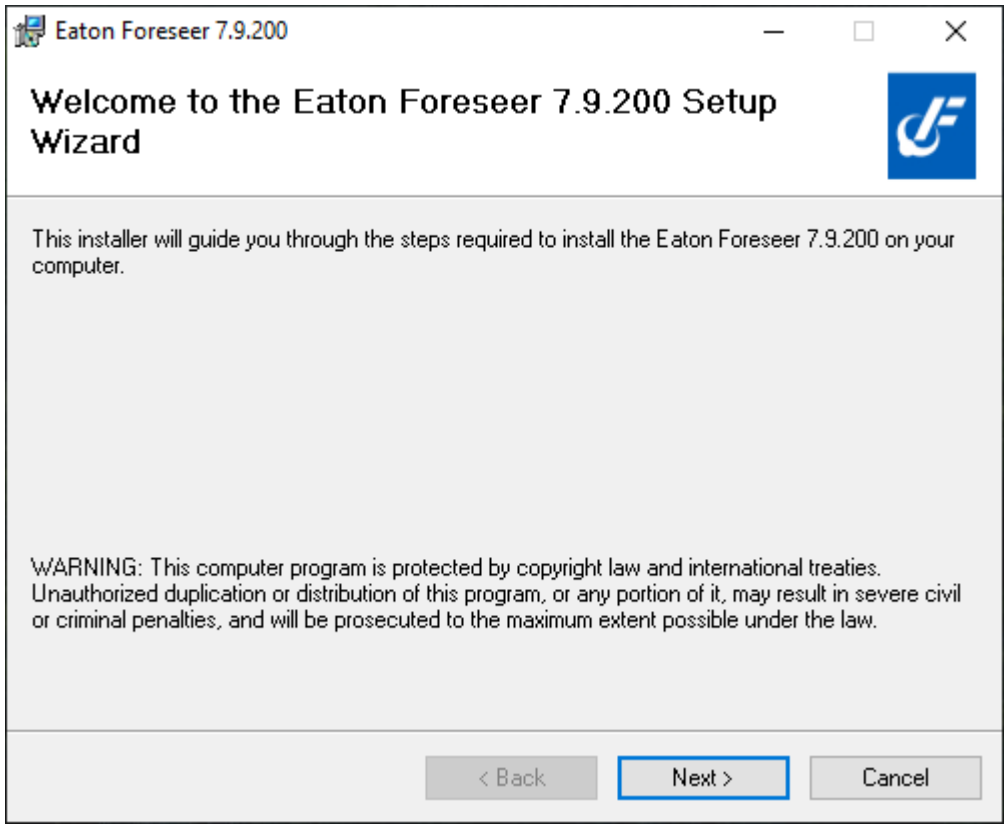
The Foreseer Server Application installation is performed from the electronic distribution and includes all of the required files. You are prompted for the drive destination and the application is placed in the specified location. There are two installation .MSI files located in the Installer folder:

- The ForeseerInstaller.msi - This is the installer for the Foreseer application.
- The MsgManInstaller.msi - This can be installed on the location machine, or even a remote server if needed. This can be a good strategy as it allows the message manager to respond should the Foreseer server be down. If you do this, you'll need to configure the Message Manager on the client machine to point to the Foreseer server (covered in the Message Manager Client Setup Guide) and configure the Foreseer Server to accept

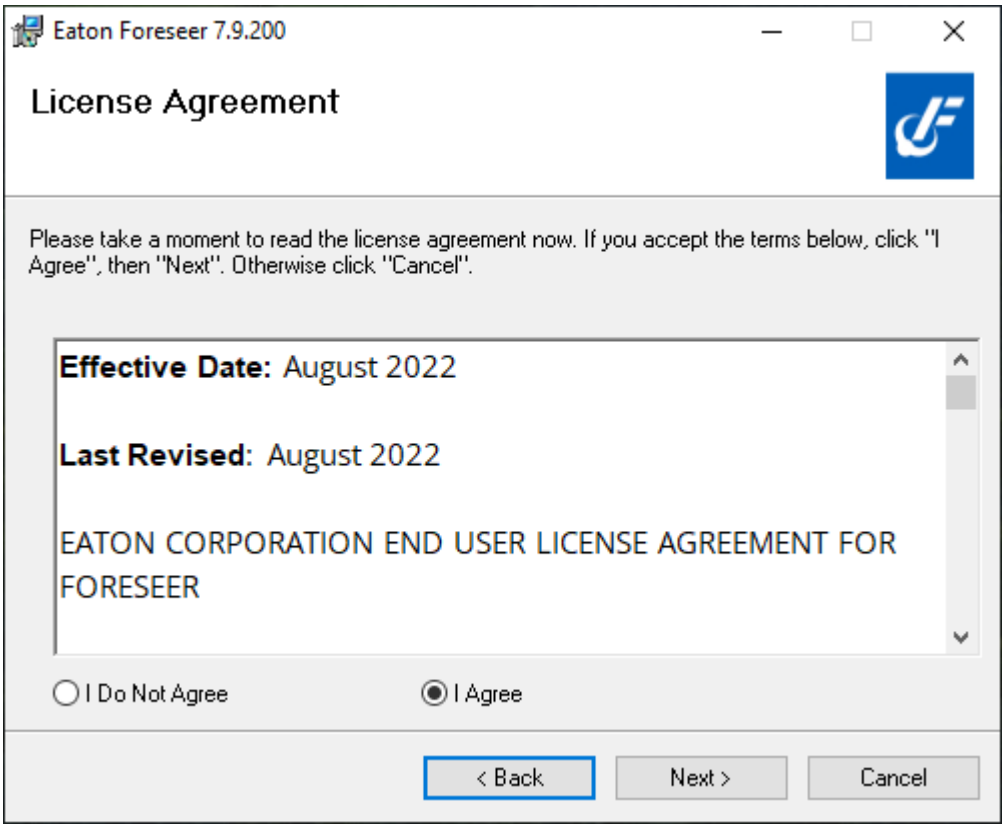
connections from this client.

Installing the Server software

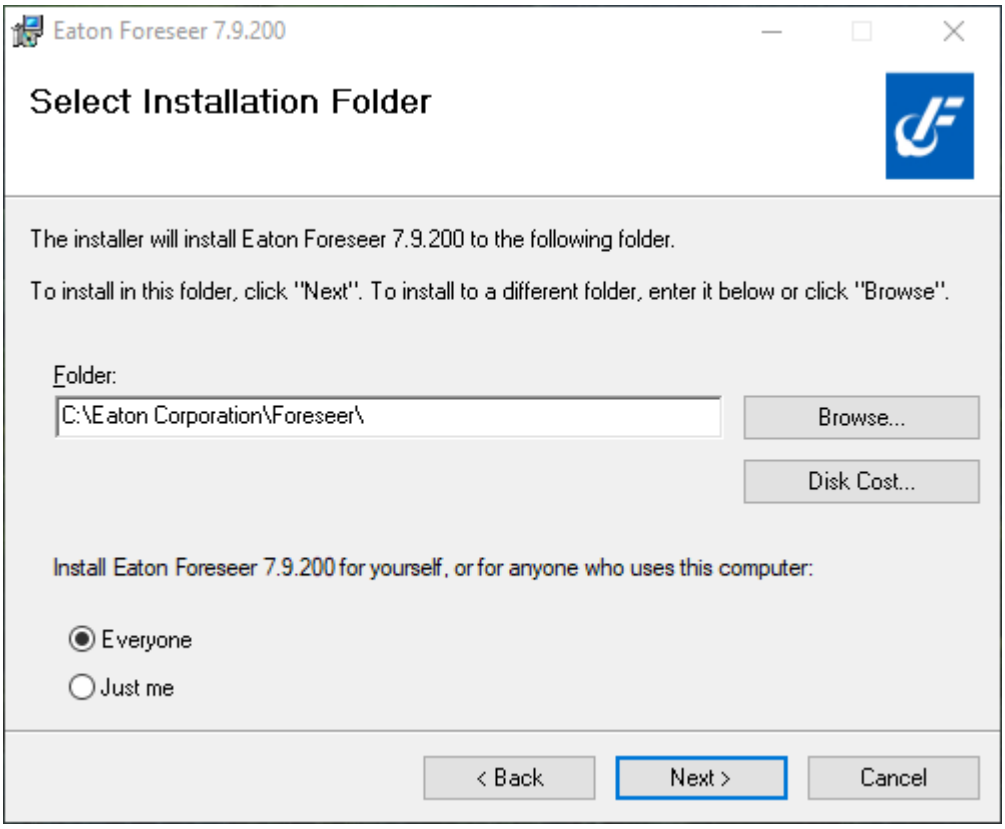
1. Launch the Windows File Explorer.
2. Browse to locate the Foreseer installation file (ForeseerInstaller.msi) on the Foreseer Server Application ISO, and then double click the install file to begin the installation. A Welcome dialog box is presented. Click *Next* to continue.



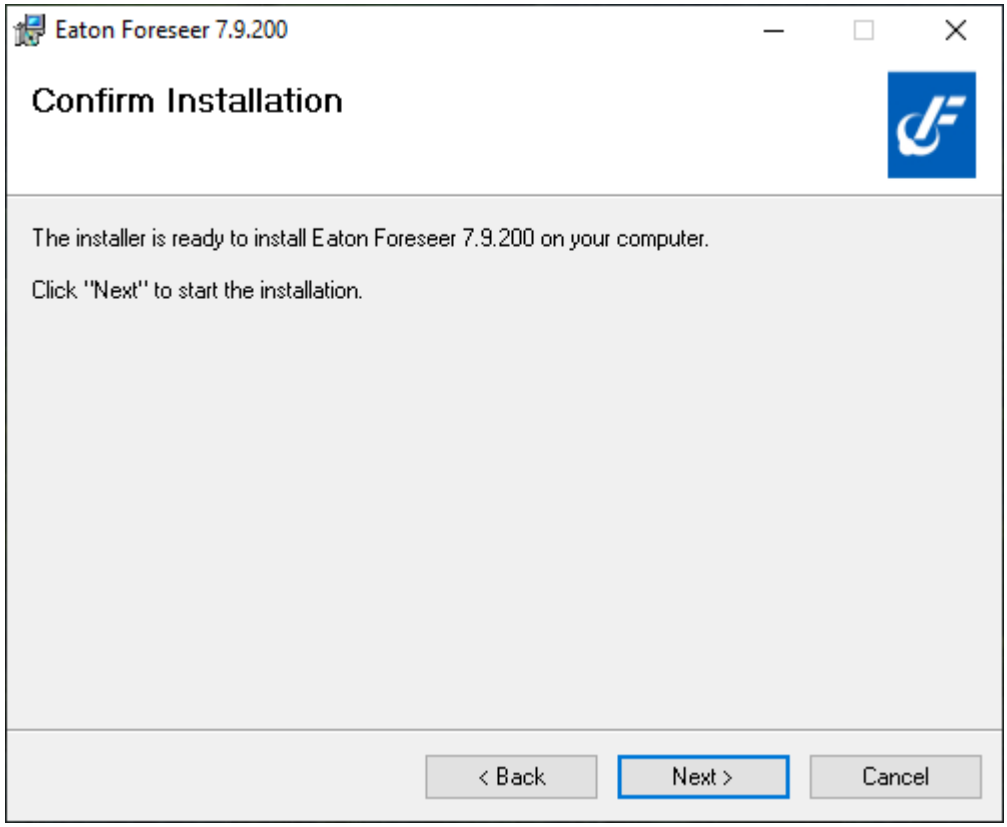
3. To install Foreseer, you must agree to the terms set forth in the License Agreement. Please review the information carefully. Once you are in agreement, click the I Agree radio button and click *Next* to continue.



4. On the Select Installation Folder screen, enter the directory location where the Foreseer application should be installed and select if the install should be for “Everyone” or for the current user. Click *Next* to continue.

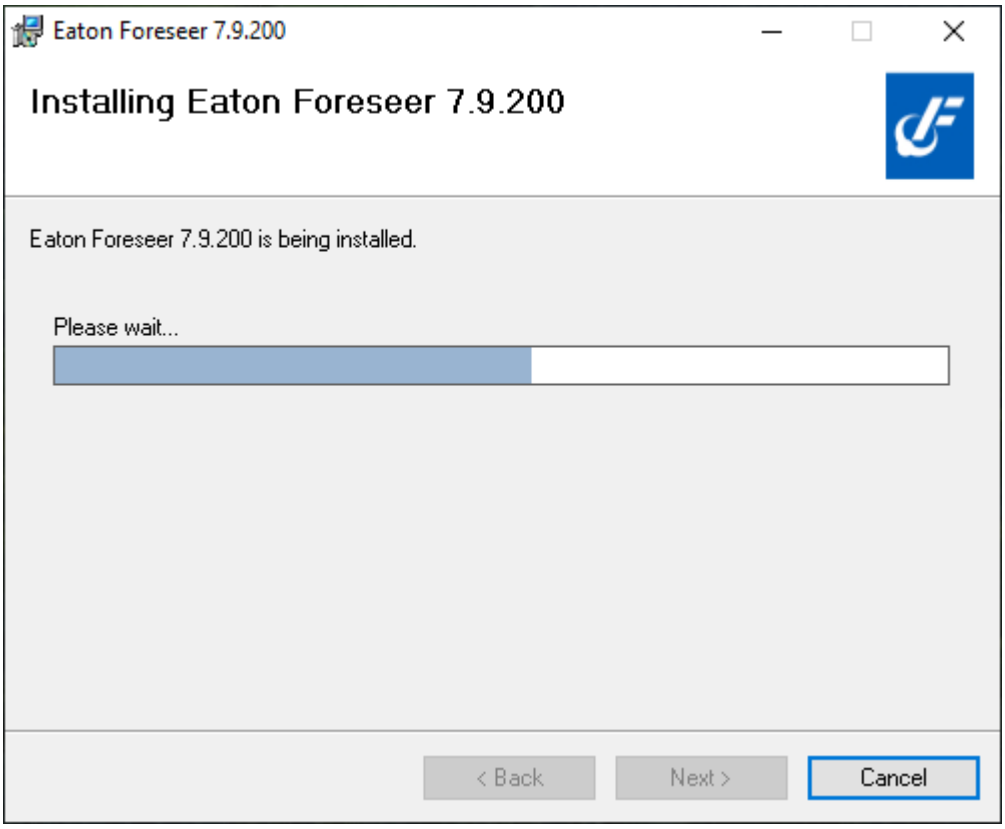


5. On the Confirm Installation screen, click *Next* to continue or *Back* to modify any of the installation settings.

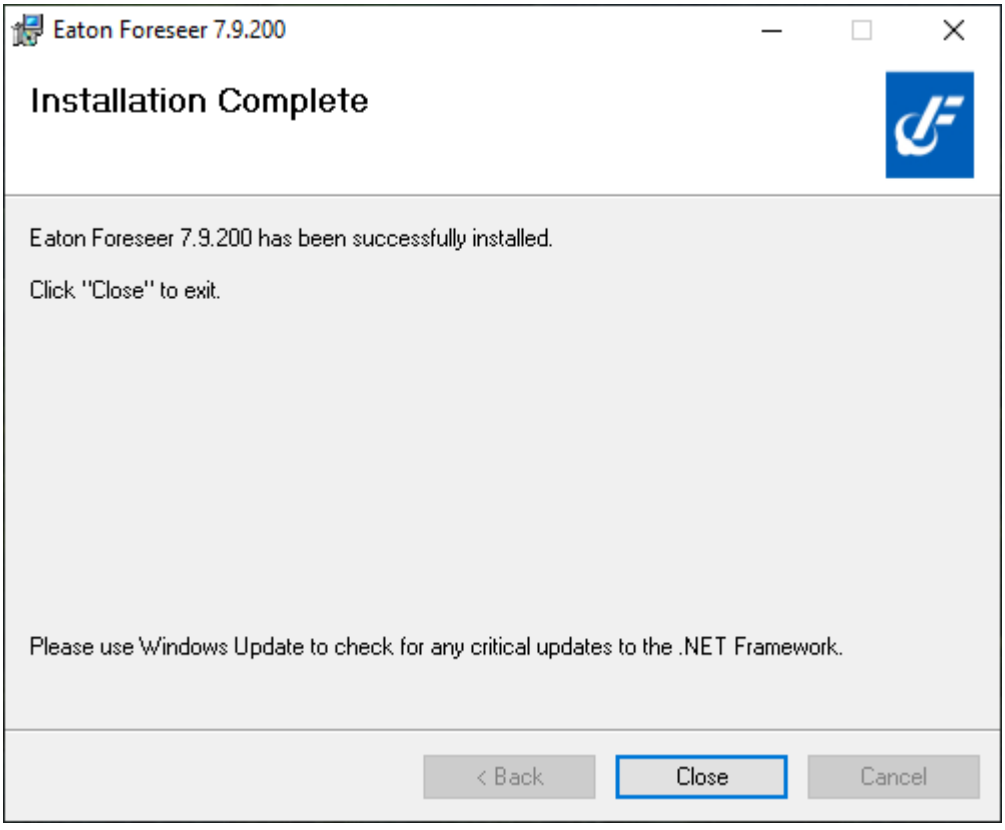


Security dependent, you may encounter User Account Control confirmation messages during setup. Be sure to click Yes to allow the installer to make necessary changes.

6. The installer will provide progress of the overall installation. This process may take a few minutes.



7. The Install Completed screen appears upon successful completion of the installation. Click **“Close”** to exit the wizard.



The installer will create a Foreseer program group in the Windows Start menu that includes the following:

Device Configuration - Launches the Device Configuration utility, which you can use to add devices to a running Foreseer Server service and change channel message settings for Message Management.
Foreseer - Launches the Foreseer Server itself.

8. Once the installation is complete, you may be prompted to restart the system. Click **"Yes"** to restart your system if prompted.
9. From the *Sql Client Tools* folder located in your Foreseer installation, run the msoledbsql_18.3.0.0_x64.msi and MsSqlCmdLnUtils.msi installation files to ensure that Foreseer can communicate local and remote SQL Server instances.

    1. MsSqlCmdLnUtils.msi likely will require msodbcsql.msi as a prerequisite.

> Failure to install the .msi files in the *Sql Client Tools* directory may result in Foreseer not communicating with a local or remote SQL Server instance.

9. Install the Microsoft Visual C++ Redistributable provided with this release.
    1. These files are in ./Foreseer/Applications/VCRedist folder.
    2. Install the appropriate redistributable file for your system type.
        1. vcredist_x64.exe or vcredist_x86.exe

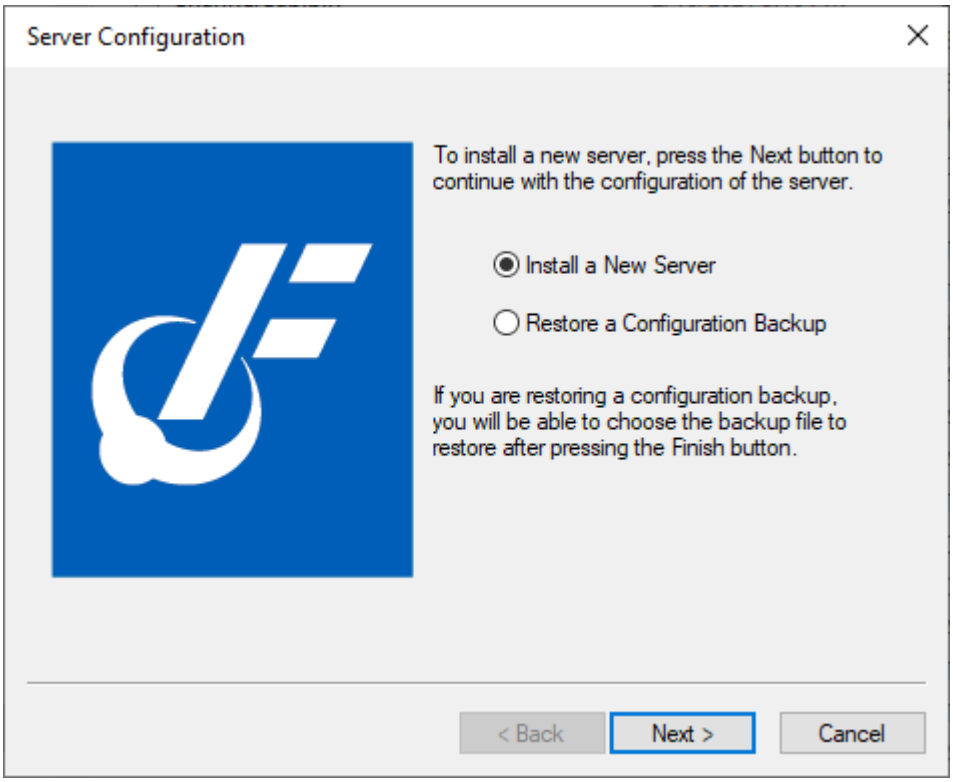
Configuring the Server

The initial step in setting up Foreseer is to configure the Server. This includes establishing password authorization, if desired, to protect the basic administrative operations governing the maintenance of the application.

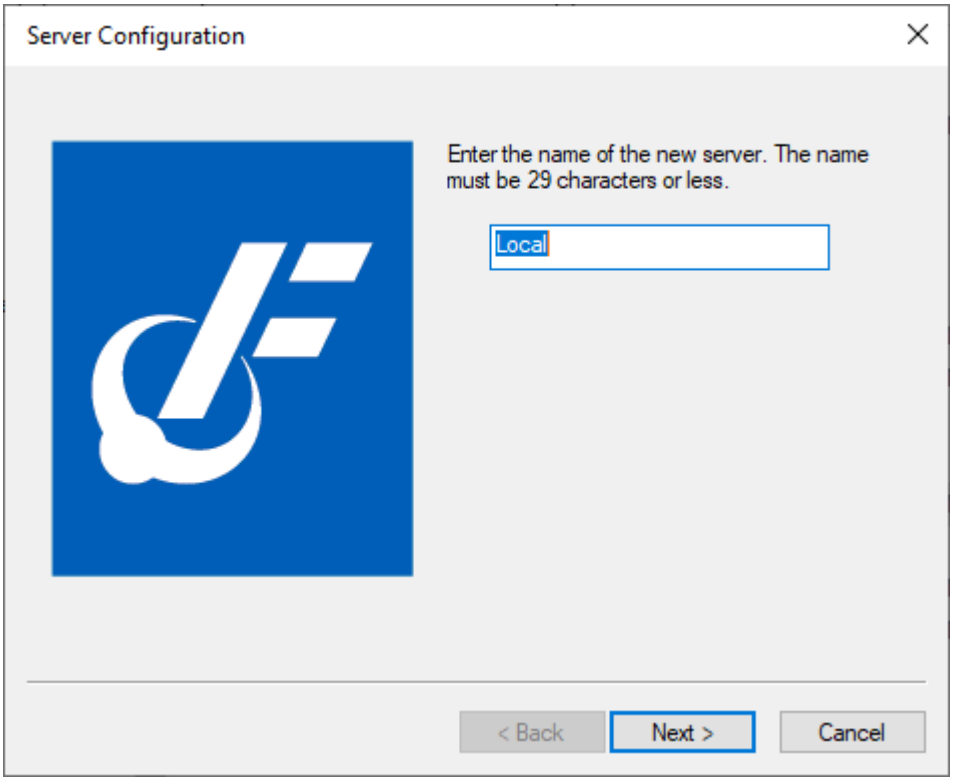
Installing a New Server

Launch the Foreseer server by selecting Start > All Apps > Foreseer > Foreseer Server.

1. In the Server Configuration Wizard dialog box, select "Install a New Server" and click **"Next"** to continue

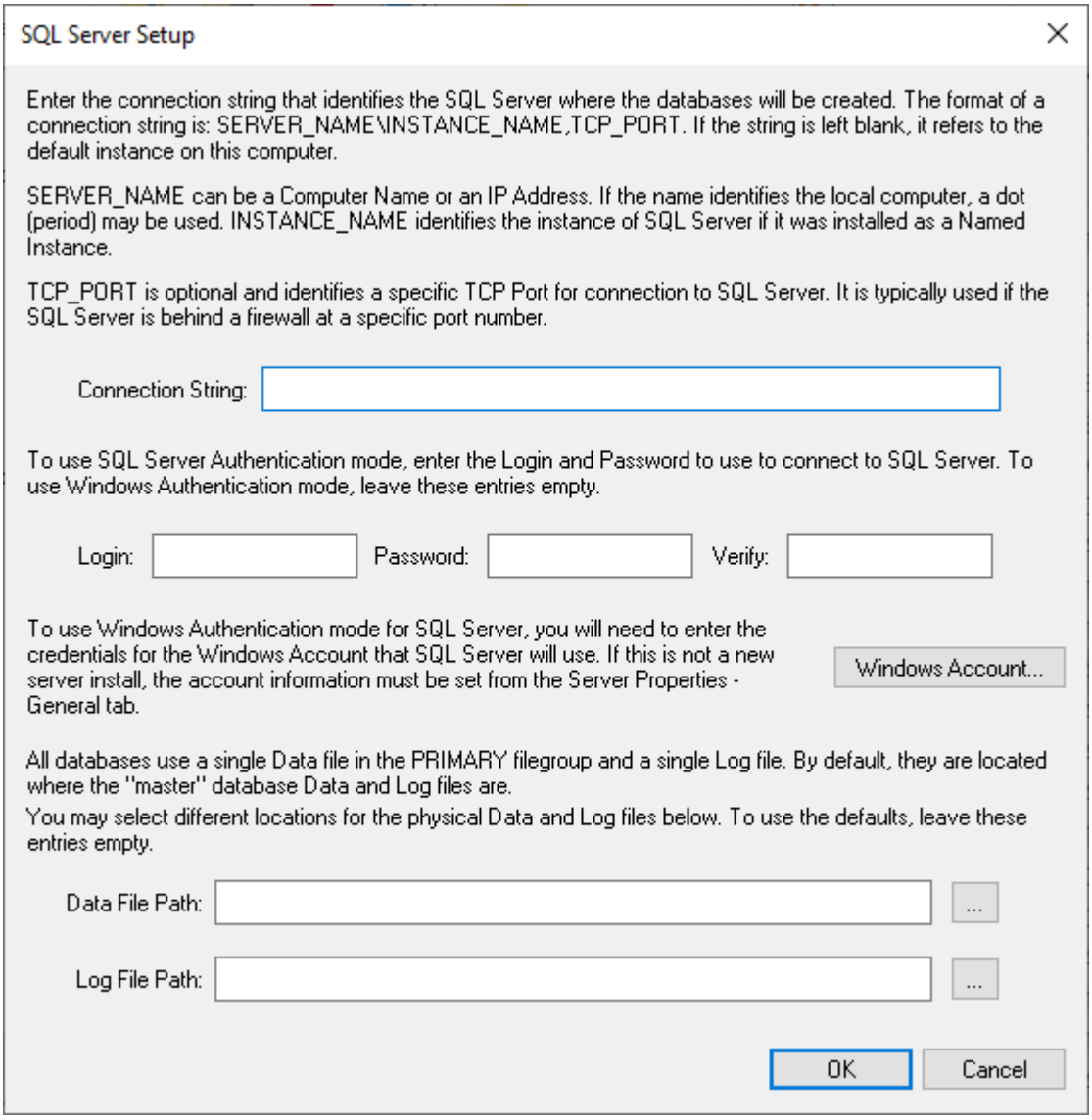


2. Make sure a Configuration Checklist at the back of this manual has been completed for each of the connected Devices.
3. On the Server Configuration screen, identify this Foreseer Server for communication and reporting purposes by typing in a name, up to 29 characters. Click **"Next"** to continue with the Server configuration.

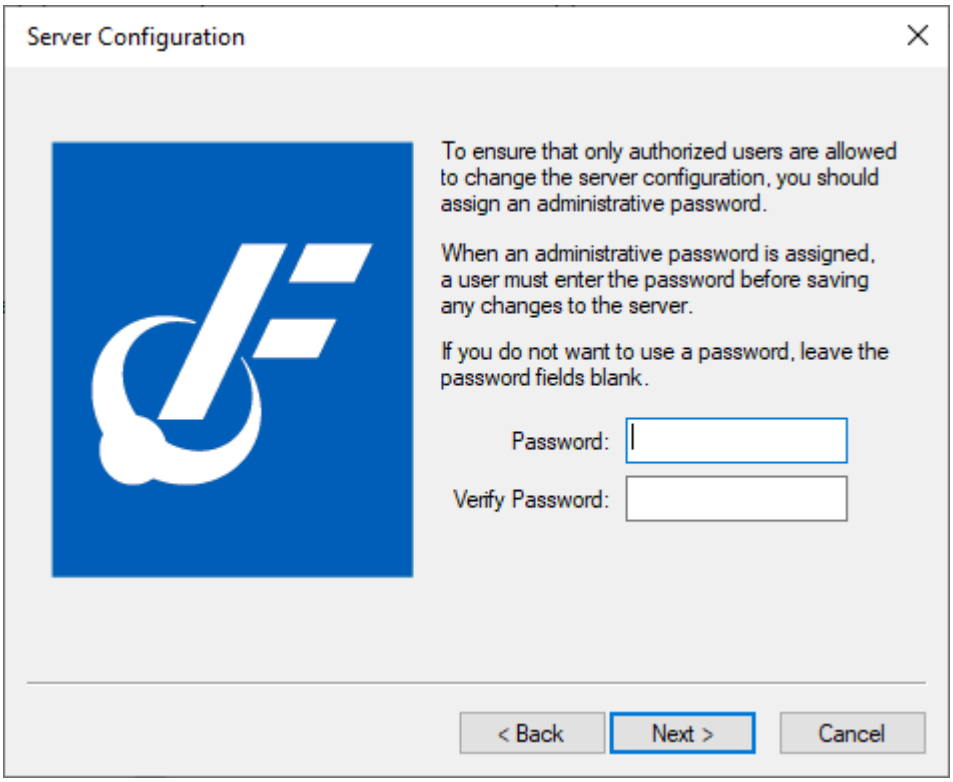


4. On the SQL Server Setup screen, specify the Database File and Transaction Log

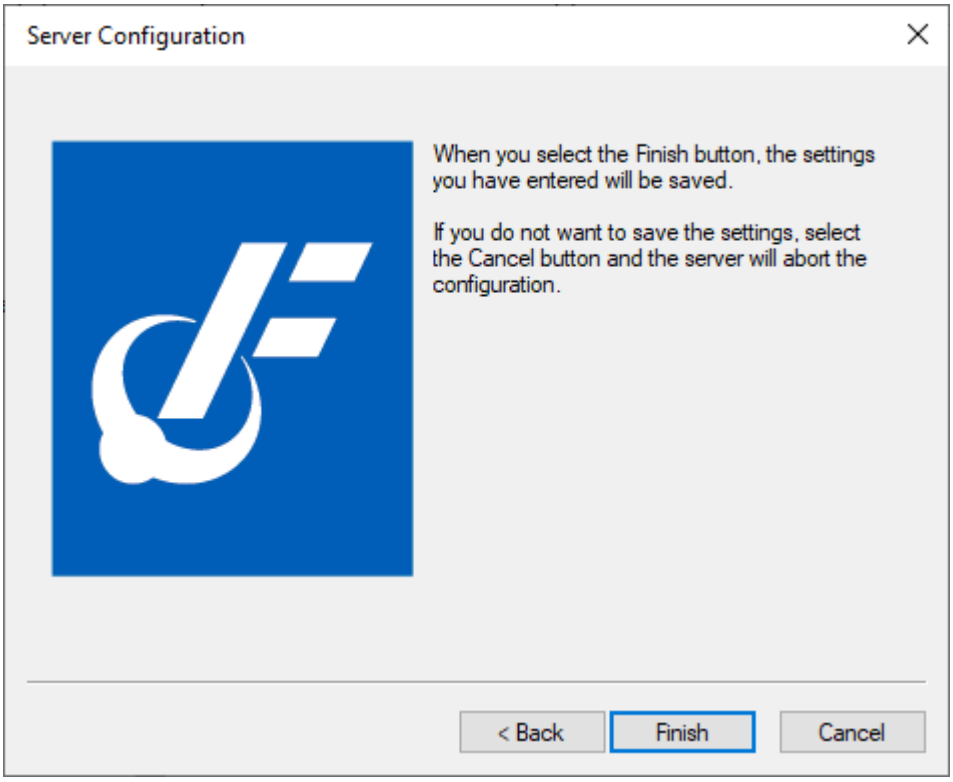
Locations, if desired. With the necessary SQL Server information entered, click “Next” to continue.



5. On the Server Configuration / Password screen, you may optionally require password authorization before changes can be made to the Server. Password protection is recommended in critical installations to prevent inadvertent changes which could adversely affect the system. Please be sure to record the password and store it in a safe location. Again, you must enter the Password in both fields to confirm it. Click **“Next”** to continue.



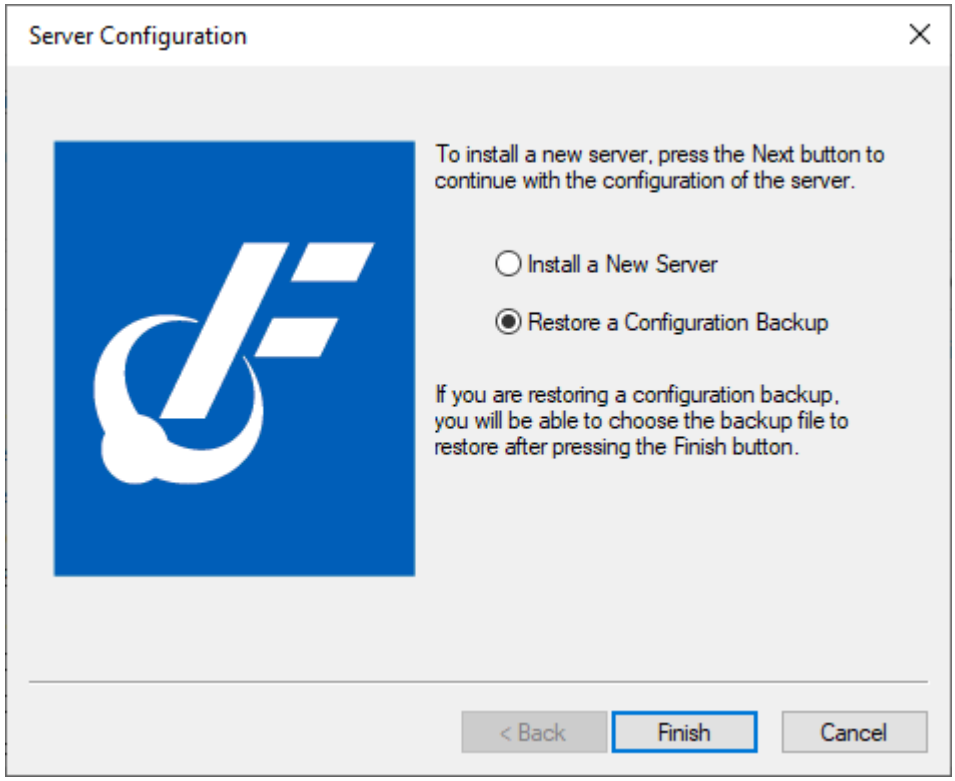
6. On the Server Configuration / Finish screen, click **"Back"** to change any of the chosen setup parameters, if necessary, otherwise, click **"Finish"** to save the Server Configuration settings. The Foreseer Server software is launched automatically.



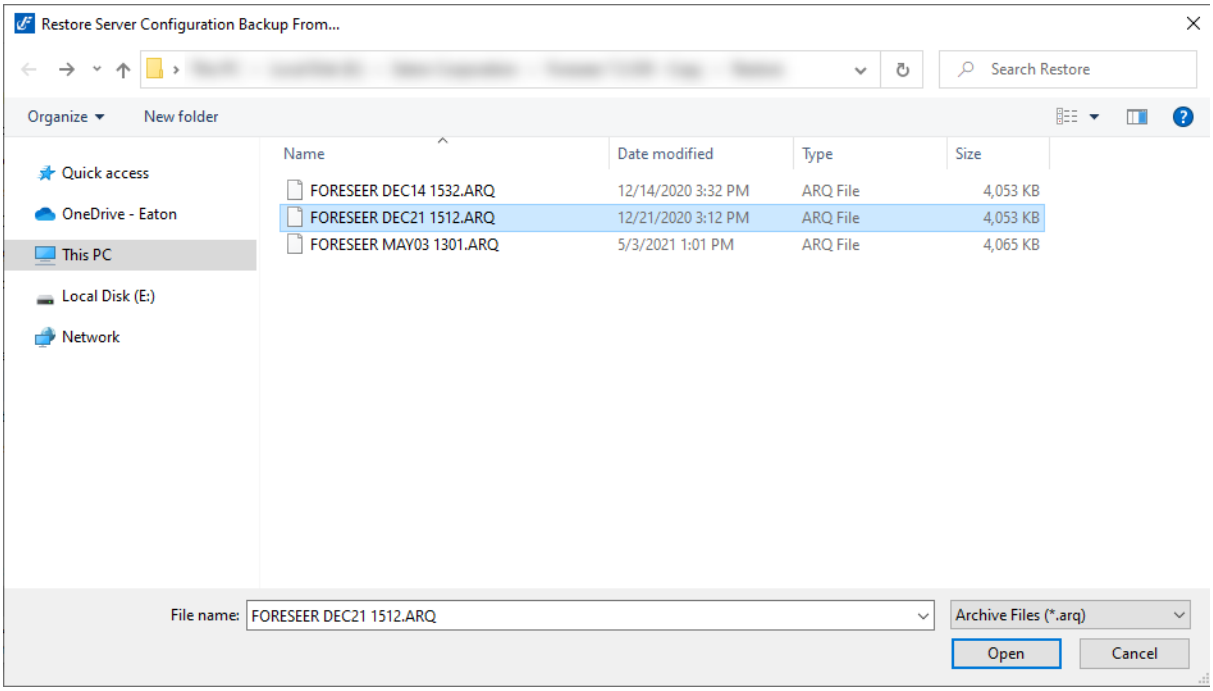
To Restore a Configuration Backup

Launch the Foreseer server by selecting Start > All Apps > Foreseer > Foreseer Server.

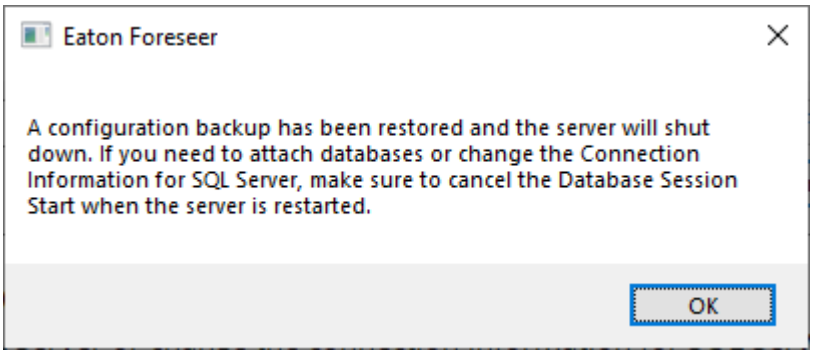
1. In the Server Configuration Wizard dialog box, select “Restore a Configuration Backup” and click **“Finish”** to continue



2. Make sure a Configuration Checklist at the back of this manual has been completed for each of the connected Devices.
3. The Restore Server Configuration Backup From... dialog will open up. Select the Foreseer ARQ that you want to restore.



4. Once the ARQ file has been restored, the Eaton Foreseer Confirmation Dialog will be displayed.
    1. Select “Yes” if you need to attach databases to SQL Server or change the connection information for SQL Server.
    2. Select “No” if you do not need to change the SQL Server properties and your current databases are already attached. The server will start up and will run an automatic Fix Databases command.



Once the Foreseer program installation is complete, refer to the Foreseer application’s help files for further instructions.

- Server Guide CHM Help File
- Device Configuration Utility Guide PDF File

Web Server Configuration

By default, the Foreseer Web Server operates in the following manner:

- Secure HTTP only access (via HTTPS) via Port 443
- Enabled for TLS v1.3 and TLS v1.2 encryption with secure protocol ciphers

- Auto-generated self-signed certificate for start-up purposes
- Default allow list configuration granting access to all browser addressed clients

Users can override the default behavioral settings of the Foreseer Web Server through two mechanisms.

User Web Server Configuration

The default behavior of the Foreseer Web Server can be modified through the use of a user_httpd.conf file. When installed, Foreseer will create this file with an .example file extension (e.g. user_httpd.conf.example) in the WWW directory of your install (normally C:\Eaton Corporation\Foreseer\WWW).

```
##############################################################################
#
# user_httpd.conf - Site specific settings for Apache configuration.
#
# This file will be included in a configuration backup (a .arq file)
# and will be restored when a 7.1.160 or later backup file is restored.
# You can check any modifications to this file by running Apache with
# the -t switch as follows:
#
#    ...installPath\Apache24\bin\httpd.exe -t
#
# If the syntax is accecptable, it will display "Syntax OK". If not,
# an error message will be displayed with the line number in the file.
#
##############################################################################

##############################################################################
# The port that the TLS enabled secure server will listen on:
#
#Define HTTPS_PORT 443

##############################################################################
# The default auto-generated certificate file name and the private
# key file name. Site supplied certificates can be either PEM encoded
# or ASN1 (DER) encoded. Either server.crt or server.pem (server.csr is
# allowed but not recommended) may be used. The site supplied private
# key file name must always be server.key. To use your own certificate
# and key, copy the files to the ...installPath\Certs folder and
# uncomment following line (change name to "server.pem" if your
# certificate file extension is .pem).
#
#Define CERTIFICATE_NAME "server.crt"


##############################################################################
# The default TLS protocol and cipher suite strings
#
# TLS_PROTOCOLS is used to enable TLS server protocol support.
#
# CIPHER_SUITES is used to configure TLSv1.2 supported ciphers.
#
# CIPHER_SUITES_TLSv1_3 is used to configure TLSv1.3 supported ciphers.
#
#Define TLS_PROTOCOLS "-all +TLSv1.3 +TLSv1.2"
#Define CIPHER_SUITES "ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!NULL:!RC4:!RC2:!DES:!3DES:
#Define CIPHER_SUITES_TLSv1_3 "TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:'
```

The example file can be adjusted using any text editor and renamed with the .example extension removed to make changes effective upon restarting the Eaton Foreseer Apache Service. To override a specific parameter, remove the comment (#) from the beginning of

the parameter definition.

user_httpd.conf Settings	
Parameters	**Notes**
HTTP_PORT	By default, the Foreseer Apache Service will not permit connectivity over un-secure HTTP access. While this feature continues to be available for user configuration for legacy reasons, it is strongly recommended that you do not enable un-secure HTTP access.
HTTPS_PORT	By default, the Foreseer Apache Service is available on Port 443 for HTTPS access. If you plan to access Foreseer web applications on a lesser known port, remove the comment marker and ensure enter a desired port assignment.
CERTIFICATE_NAME	By default, the Foreseer Apache Service will utilize the autoGen.crt file generated by Foreseer upon start-up. If you plan to install your own CA-generated certificate, remove the comment marker and ensure that the name of your certificate is either server.crt or server.pem
TLS_PROTOCOLS	By default, the Foreseer Apache Service will not support all protocols, rather, exclusively support TLS v1.3 and TLS v1.2 protocols. To deviate from this default behavior, remove the comment marker and remove the protocol definition. Note that the "-all" marker is used to ensure that only the protocols listed with a "+" marker are supported.
CIPHER_SUITES	By default, the Foreseer Apache Service will support only HIGH and MEDIUM ciphers for TLS v1.2. Advanced users that need to adjust the cipher suite behavior defined here can remove the comment marker and edit as necessary. This token follows Apache standard for the SSLCipherSuite configuration. For more details, refer to the following link: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslciphersuite
CIPHER_SUITES_TLS_1_3	By default, the Foreseer Apache Service supports secure and recommended ciphers for TLS v1.3. Advanced users that need to adjust the cipher suite behavior defined here can remove the comment marker and edit as necessary. Pay special attention to the fact that TLS 1.3 ciphers are defined in a colon delineated format and do not support classic re-negotiation parameters observed in the CIPHER_SUITES parameter used to control TLS v1.2 protocol. This token follows Apache standard for the SSLCipherSuite configuration for TLS v3. For more details, refer to the following link: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslciphersui

	te

User Web Server Allow List Configuration

The default behavior of allowed client access can be modified through the use of a user_allowlist.conf file. When installed, Foreseer will create this file with an .example file extension (e.g. user_allowlist.conf.example) in the WWW directory of your install (normally C:\Eaton Corporation\Foreseer\WWW). This file utilizes Apache's Require directive to ensure that a client is allowed or denied access to the web server.

```
# INSTRUCTIONS
#
# By default, all clients can access the Foreseer web server.  If you
# wish to restrict capabilities to specific clients, you can list
# clients by IP address or hostnames.  Ranges of IP address using CIDR
# notation is supported, as well as wildcards for hostnames.
#
# A default installation Foreseer will allow all clients to connect to
# the webserver using the single "Require all granted" entry.  Removal
# of this entry is required to omit/restrict connections only to defined
# clients in this configuration file.
#
# NOTE:  If you plan to use FRS and remove the default all granted entry,
# add a listing for "Require local".  This allows the reverse
# proxy feature to connect to the FRS Core Web engine (see example below).
#
# Full documentation of require directives can be found at
# https://httpd.apache.org/docs/2.4/mod/mod_authz_host.html#reqip
#
#----------------------------------------------
# Examples:
#
# single ip
# Require ip 10.1.2.3
#
# partial ip wildcard
# Require ip 10.1
# Require ip 10.172.20
#
# network/netmask pair
# Require ip 10.1.0.0/255.255.0.0
#
# network/nnn cidr specification
# Require 10.1.0.0/16
#
# hostname
# Require host example.org
#
# localhost access
# Require local
#
#----------------------------------------------
#
##############################################################################

Require all granted
```

By default, the file contains the "Require all granted" definition, which permits all clients with access to the web server. The example file can be adjusted using any text editor and renamed with the .example extension removed to make changes effective upon restarting

the Eaton Foreseer Apache Service.

The file permits access to clients that meet the specifications defined within this file. Clients that do not meet the specifications outlined within this file will not be granted access.

Require ip

The Require ip provider allows access to the server to be controlled based on the IP address of the remote client. When Require ip is specified, then request to the web server are allowed access if the IP address matches. Examples of this include:

A full IP address can be a single address or a list of space delimited addresses on a single line:

```
Require ip 10.1.2.3
Require ip 192.168.1.104 192.168.1.205
```

A partial IP address, essentially allowing for subnet restrictions or "wildcard" access:

```
Require ip 10.1
Require ip 10 172.20 192.168.2
```

A network/netmask pair:

```
Require ip 10.1.0.0/255.255.0.0
```

A network/nnn CIDR specification:

```
Require ip 10.1.0.0/16
```

A definition similar to the above, but applicable to IPv6 addressing:

```
Require ip 2001:db8::a00:20ff:fea7:ccea
Require ip 2001:db8:1:1::a
Require ip 2001:db8:2:1::/64
Require ip 2001:db8:3::/48
```

Require host

The Require host provider allows access to the server to be controlled based on the host name of the remote client. When Require host is specified, then requests to the web server are allowed access if the host name matches. This is useful for partial domain name access.

```
Require host example.org
Require host .net example.edu
```

Hosts whose names match, or end in, the above would be allowed access. Only complete components are matched, so the above example will match *foo.example.org*, but it will not match *fooexample.org*. This configuration will cause the Foreseer Apache web server to perform a double reverse DNS lookup on the client's address. It will do a reverse DNS lookup on the IP address to find the associated hostname, and then do a forward lookup on the hostname to assure it matches the original IP address. Only if the forward and reverse DNS are consistent and the hostname matches will access be allowed.

Require forward-dns

The forward-dns provider allows access to the server to be controlled based on simple host names. When Require forward-dns is specified, all IP addresses corresponding to the defined host name are allowed access.

In contrast to the host provider, this provider does NOT rely on reverse DNS lookups. It simply queries the DNS for the host name and allows a client if its IP matches. As a consequence, it will only work with host names, not domain names. However, as the reverse DNS is not used, it will work with clients which use a dynamic DNS service.

```
Require forward-dns dynamic.example.org
```

A client the IP of which is resolved from the name dynamic.example.org will be granted access in the example shown above.

Require local

The local provider allows access to the server if any of the following conditions are true:

- The client address matches 127.0.0.0/8
- The client address is ::1
- Both the client and the server address of the connection are the same.

This allows a convenient way to match connections that originate from the local host - especially in server deployments where Foreseer Reporting Services is added on.

```
Require local
```

Server Upgrade

To Upgrade from Foreseer 6.3.172, Foreseer 7.x

Upgrade Steps

1. Thoroughly review existing v6.3 or v7.x System:

1. Run a Check Databases. Follow with a Fix Databases if any inconsistencies are found. Work with CST if necessary, to correct any issues with the database.
2. Generate a Log Report file for errors. IF any are presented, they must be corrected before upgrading. Look carefully for any entries with “ERROR” or “WARNING”.
3. Restart Foreseer and generate a new Log Report. Verify that no derived equation parsing errors are listed at the beginning of the new log file. Work with CST if necessary, to correct all errors and equations that may exist.
4. Note your current SQL Connection String, credentials, and file paths.
5. Generate a System Configuration Report.
6. Note any devices that are not communication and correct if possible.
7. Generate a new system configuration backup (ARQ) if changes were necessary to correct errors.

2. Create System Configuration Backup (ARQ)

    1. Create a new System Configuration Backup (ARQ) of the existing system. You can do this by executing the “Config Backup” command in WebConfig or by running Foreseer as an application and performing a configuration backup from there.
    2. ARQ backups can be located in the Restore directory of your Foreseer installation – typically C:\Eaton Corporation\Foreseer\Restore.

3. Obtain Updated Driver DLLs

    1. Open and review the System Configuration Report from Step 1-E. Make a list of all driver DLLs currently in use.
    2. Access the Foreseer file server and obtain the latest driver DLLs for use with Foreseer. These can be found at the following location:
        1. \\simtcnas002\lafcosfp01\shared\Manufacturing\
    3. Store a copy of these updated driver DLLs; they will be needed in steps to follow within this document.

4. Uninstall the Foreseer Windows Service

    1. You must uninstall the Foreseer service using the existing ServiceSetup.exe application typically located in C:\Eaton Corporation\Foreseer.
    2. Verify that the Windows Administrative Tools>Services no longer contains Eaton Foreseer. If you are updating from a prior revision of v7, verify that the Foreseer Apache or Eaton Foreseer Apache service no longer exists. A server reboot may be necessary.

5. Install Foreseer

    1. *Option 1*: Install in a new directory; providing a simple back-out plan to revert to version 6.3.172 if needed.

2. *Option 2:* Un-install existing versions first, then install new version afterwards.

Option 1 – Install Foreseer Into New Folder

1. Run the ForeseerInstaller.msi and specify a new path for installation – such as C:\Eaton Corporation\Foreseer.
2. The installation process will update all Windows Shortcuts. If running Foreseer as an application, the Windows Start Menu links will update.
3. Run the msoledbsql_18.3.0.0_x64.msi file located in the SQL Server Client Tools folder of your Foreseer installation.
4. Start Foreseer as an application.
5. Select Restore a Configuration Backup. Browse to the ARQ created in Step 2A.
6. When prompted whether to shut-down or re-attach databases, select "No". Foreseer will perform the necessary database activities to re-link the configuration to the existing databases. The ARQ will also be updated to a v7.4 compliant format.
7. Shutdown the Foreseer application.
8. Update the driver DLL files in the VI directory as noted in Step 3 to the current version of the drivers.
9. Navigate to the \Data\ directory of your Foreseer installation. Delete the RemoteBufferedData.srv and RemoteBufferedData.bak files if they exist.
10. Restart Foreseer as an application and verify general device communications.
11. Shutdown the Foreseer application.
12. Run the ServiceSetup.exe utility from the installation path you selected earlier. Install both the Foreseer and Apache services. Go to Administrative Tools>Services and configure both services to run with the appropriate Log On service account.
13. Using Windows Explorer, access C:\Eaton Corporation\Foreseer\WWW. Locate the *user_httpd.conf.example* file. Open this file with a text editor.
14. Edit the following lines for your WebViews server:
    1. Line 22 – Remove comment symbol (#), and specify the port used for HTTP connectivity if desired. The default is Port 80.
    2. Line 27 – Remove comment symbol (#), and specify the port used to HTTPS connectivity. The default is Port 443.
    3. Line 39 – Remove comment symbol (#) if the customer has

already supplied their own SSL Certificate. If the customer has not issued their own certificate, leave the comment symbol in to use a self-signed certificate automatically generated by Foreseer.

4. Line 45 – Remove comment symbol (#).
5. Line 46 – Remove comment symbol (#).

15. Save the *user_httpd.conf.example* file.
16. Rename the *user_httpd.conf.example* file to **user_httpd.conf**.

If the customer is using their own server certificate, the name the corresponding private key file MUST be server.key.

Neglecting to rename the file as described above will result in the Eaton Foreseer Apache service initializing with default parameters (HTTPS over 443 and use of self-signed autoGen certificate files from the Certs directory)

17. Start the Foreseer service. Once started, the Eaton Foreseer Apache service should automatically start as well. You may need to Refresh the Services application in order to see the service status change.
18. Generate a log file from WebConfig and make sure that all devices are initializing and there are no errors or warnings. If necessary, consult CST for assistance with resolving any issues.

Option 2 – Uninstall Old Rev, Install New Rev into Same Folder

1. Locate, determine, and note the existing Foreseer installation path – typically C:\Eaton Corporation\Foreseer.
2. Use Control Panel's Programs and Features application to uninstall the current revision of Foreseer.
3. Run the ForeseerInstaller.msi and specify the same path.
4. Run the msoledbsql_18.3.0.0_x64.msi file located in the SQL Server Client Tools folder of your Foreseer installation.
5. Navigate to the \Data\ directory of your Foreseer installation. Delete the RemoteBufferedData.srv and RemoteBufferedData.bak files if they exist.
6. Launch Foreseer as an application. Allow the program to update the existing ARQ. You will be notified that the document upgrade has completed, and that the server will exit.
7. Update the driver DLL files as noted in Step 3 to the current version of the drivers.

8. Verify general device communications. If necessary, consult CST to resolve any issues.

9. Run the ServiceSetup.exe utility from the installation path you selected earlier. Install both the Foreseer and Apache services. Go to Administrative Tools>Services and configure both services to run with the appropriate Log On service account.

10. Using Windows Explorer, access C:\Eaton Corporation\Foreseer\WWW. Locate the *user_httpd.conf.example* file. Open this file with a text editor.

11. Edit the following lines for your WebViews server:

    1. Line 22 – Remove comment symbol (#), and specify the port used for HTTP connectivity if desired. The default is Port 80.

    2. Line 27 – Remove comment symbol (#), and specify the port used to HTTPS connectivity. The default is Port 443.

    3. Line 39 – Remove comment symbol (#) if the customer has already supplied their own SSL Certificate. If the customer has not issued their own certificate, leave the comment symbol in to use a self-signed certificate automatically generated by Foreseer.

    4. Line 45 – Remove comment symbol (#).

    5. Line 46 – Remove comment symbol (#).

12. Save the *user_httpd.conf.example* file.

13. Rename the *user_httpd.conf.example* file to **user_httpd.conf**.

    1. NOTE – If the customer is using their own server certificate, the name the corresponding private key file MUST be *server.key*.

14. Start the Foreseer service. Once started, the Eaton Foreseer Apache service should automatically start as well. You may need to Refresh the Services application in order to see the service status change.

15. Generate a log file from WebConfig and make sure that all devices are initializing and there are no errors or warnings. If necessary, consult CST for assistance with resolving any issues.

6. Complete the Upgrade

    1. Review WebViews and WebConfig for general functionality and content.

    2. Create a System Configuration Backup of the newly upgraded system.
        1. Please name the file according to the following format:
            1. Customer-Site-V7-Server-MMDDYY-Field.ARQ
            2. Example: XYZCompany-Chicago-V7-Server-031214-Field.ARQ
    3. Send the link to the ARQ file (Box.com, Hightail.com, Dropbox.com, Eaton FTP, Common) to GUI for permanent archiving

Roll Back Procedure

> Should you encounter a fatal issue that requires the new version to be removed and revert to the previous revision, follow this procedure.
>
> An ARQ from a newer revision of Foreseer is not backwards compatible with prior Foreseer software versions.

1. Stop the Eaton Foreseer Server Service. The Eaton Foreseer Apache Service should stop once the Foreseer service has stopped.
2. Run ServiceSetup.exe located in the Foreseer v7.x.xxx path. Uninstall both the Eaton Foreseer and Eaton Foreseer Apache services. Verify that Administrative Tools>Services no longer contains an entry for either service. A reboot may be necessary.
3. Go to Control Panel>Programs and Features. Find Eaton Foreseer and select Uninstall.
4. After the uninstall process has completed, remnant configuration files may be present in the directory where Foreseer resided. These files should be deleted or moved to an alternate location to prevent confusion.
5. For Option 1 installation scenarios:
    1. Run Foreseer.exe from the installation directory where the previous installation resides. Verify that all devices are communicating. Verify general functionality and run a Log Report if necessary.
    2. Run ServiceSetup.exe and install the Eaton Foreseer services Start the service in Administrative Tools>Services.
    3. Verify general WebViews and WebConfig functionality.
6. For Option 2 installation scenarios:
    1. Uninstall the new revision of Foreseer.
    2. Install your previously used revision of Foreseer and follow the installation wizard steps.
    3. Start Foreseer.exe and restore your archived ARQ.
    4. Once the ARQ has been restored, verify general functionality and run a Log Report if necessary.
    5. Run ServiceSetup.exe and install the Eaton Foreseer services. Start the service in Administrative Tools>Services.
    6. Verify general WebViews and WebConfig functionality.

To Upgrade from Outpost 6.3.172

Existing Foreseer DAE Hardware Appliance Compatibility

Eaton Outpost v7 is a 64-bit remote Foreseer node that participates in an overall EPMS architecture. This software is commonly used in DAE hardware appliances. Prior to installing or upgrading, the DAE appliance must meet certain system requirements and pre-requisite software necessary to run Outpost v7

Operating System Requirements

- Windows Embedded 10 IoT Enterprise or later

> Legacy Windows XP Embedded DAE applications are no longer supported. Contact your Eaton Sales Rep for assistance on purchasing a new DAE appliance that is compatible with Outpost v7.

Software Upgrade Pre-Requisites

DAE appliances with Windows Embedded 7 with SP1 require several software pre-requisites prior to installing Eaton Outpost v7. These pre-requisites are in the form of Windows Update KBs. DAE appliances can be connected to Windows Update to obtain most pre-requisite software.

If the DAE is used in a secured environment that forbids a connection to Windows Update, you can obtain the necessary pre-requisites needed prior to installing Eaton Outpost v7. The following table provides a summary of each software component along with download links for each file. If you need assistance with obtaining these files, please contact the Eaton Customer Success Team (cst@eaton.com).

We recommend installing the Windows Update files in the sequence order provided below.

Step #	Software Component	Offline Installer Download Link
1	NET Framework v4.7.2 or later	http://go.microsoft.com/fwlink/?linkid=863265
2	Update KB2533623	http://download.microsoft.com/download/f/1/0/f106e158-89a1-41e3-a9b5-32feb2a99a0b/windows6.1-kb2533623-x64.msu
3	Update KB2670838	http://download.microsoft.com/download/1/4/9/14936fe9-4d16-4019-a093-5e00182609eb/windows6.1-kb2670838-x64.msu
4	Update KB2729094-v2	http://download.microsoft.com/download/6/c/a/6ca15546-a46c-4333-b405-ab18785abb66/windows6.1-kb2729094-v2-x64.msu
5	Update KB2731771	http://download.microsoft.

		com/download/9/f/e/9fe868f6-a0e1-4f46-96e5-87d7b6573356/windows6.1-kb2731771-x64.msu
6	Update KB2786081	http://download.microsoft.com/download/1/8/f/18f9ae2c-4a10-417a-8408-c205420c22c3/windows6.1-kb2786081-x64.msu
7	Update KB2834140-v2	http://download.microsoft.com/download/5/a/5/5a548bfe-adc5-414b-b6bd-e1ec27a8dd80/windows6.1-kb2834140-v2-x64.msu
8	Microsoft Internet Explorer 11	http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe
9	Update KB2639308	http://download.microsoft.com/download/9/1/c/91cc3b0d-f58b-4b36-941d-d810a8ff6805/windows6.1-kb2639308-x64.msu
10	Update KB2882822	http://download.microsoft.com/download/6/1/4/6141bfd5-40fd-4148-a3c9-e355338a9ac8/windows6.1-kb2882822-x64.msu
11	Update KB2888049	http://download.microsoft.com/download/4/1/3/413321d2e-2d08-4699-a635-d9828aadb177/windows6.1-kb2888049-x64.msu

Upgrade Steps

1. Thoroughly review existing 6.3 System:
    1. Generate a Log Report file for errors. IF any are presented, they must be corrected before upgrading. Look carefully for any entries with “ERROR” or “WARNING”.
    2. Restart Foreseer and generate a new Log Report. Verify that no derived equation parsing errors are listed at the beginning of the new log file. Work with CST if necessary, to correct all errors and equations that may exist.
    3. Generate a System Configuration Report.
    4. Note any devices that are not communication and correct if possible.
    5. Generate a new system configuration backup (ARQ) if changes were necessary

to correct errors.

2. Create System Configuration Backup (ARQ)
    1. Create a new System Configuration Backup (ARQ) of the existing system. You can do this by executing the “Config Backup” command in WebConfig or by running Foreseer as an application and performing a configuration backup from there.
    2. ARQ backups can be in the Restore directory of your Foreseer installation – typically C:\Eaton Corporation\Foreseer\Restore.

3. Obtain Updated Driver DLLs
    1. Open and review the System Configuration Report from Step 1-C. Make a list of all driver DLLs currently in use.
    2. Access the Foreseer file server and obtain the latest driver DLLs for use with the new version. These can be found at the following location: \ \simtcnas002\lafcosfp01\Shared\Manufacturing\
    3. Store a copy of these updated driver DLLs; they will be needed in steps to follow within this document.

4. Uninstall the Outpost/PXbridge Windows Service
    1. You must uninstall the Foreseer service using the existing ServiceSetup.exe application typically located in C:\Eaton Corporation\Outpost.
    2. Verify that the Windows Administrative Tools>Services no longer contains Eaton Outpost/PXbridge or ForeseerApache services. A server reboot may be necessary.

5. Install Outpost
    - Option 1: Install new version in a new directory; providing a simple back-out plan to revert to version 6.3.172 if needed.
    - Option 2: Uninstall Version 6.3.172 first, then install new version afterwards.

Option 1 – Install Outpost v7 Into New Folder

1. Confirm installation of all prerequisite software for existing DAE appliance hardware.
2. Install VCREDIST_x86.exe from your DVD.
3. Install VCREDIST_x64.exe from your DVD
4. Run the OutpostInstaller.msi and specify a new path for installation – such as C:\Eaton Corporation\Outpost7.
5. The installation process will update all Windows Shortcuts. If running Foreseer as an application, the Windows Start Menu links will update.
6. Start Outpost as an application.
7. Select Restore a Configuration Backup. Browse to the ARQ created in Step 2-A.
8. When prompted whether to shut-down or re-attach databases, select “No”. Foreseer will perform the necessary database activities to re-link the configuration to the existing databases. The ARQ will also be updated to a new compliant format.
9. Shutdown the Outpost application.

10. Update the driver DLL files in the VI directory as noted in Step 3 to the current versions of the drivers.
11. Restart Foreseer as an application and verify general device communications.
12. Shutdown the Outpost application.
13. Run the ServiceSetup.exe utility from the installation path you selected earlier. Install both the Eaton Outpost and Apache services. Go to Administrative Tools>Services and configure both services to run with the appropriate Log On service account.
14. Start the Outpost service. Once started, the Eaton Foreseer Apache service should automatically start as well. You may need to Refresh the Services application to see the service status change.
15. Generate a log file from WebConfig and make sure that all devices are initializing and there are no errors or warnings. If necessary, consult CST for assistance with resolving any issues.

Option 2 – Uninstall Old Rev, Install New Rev into Same Folder

1. Confirm installation of all pre-requisite software for existing DAE appliance hardware.
2. Install VCREDIST_x86.exe from your DVD.
3. Install VCREDIST_x64.exe from your DVD
4. Locate the existing Outpost v6.3.172 installation path – typically C:\Eaton Corporation\Outpost.
5. Run the OutpostInstaller.msi and specify the same path.
6. Launch Outpost as an application. Allow the program to update the existing ARQ. You will be notified that the document upgrade has completed, and that the server will exit.
7. Update the driver DLL files as noted in Step 3 to the current versions of the drivers.
8. Verify general device communications. If necessary, consult CST to resolve any issues.
9. Run the ServiceSetup.exe utility from the installation path you selected earlier. Install both the Outpost and Apache services. Go to Administrative Tools>Services and configure both services to run with the appropriate Log On service account.
10. Start the Outpost service. Once started, the Eaton Foreseer Apache service should automatically start as well. You may need to Refresh the Services application to see the service status change.
11. Generate a log file from WebConfig and make sure that all devices are initializing and there are no errors or warnings. If necessary, consult CST for assistance with resolving any issues.

6. Complete the Upgrade
    1. Review WebViews and WebConfig for general functionality and content.
    2. Create a System Configuration Backup of the newly upgraded v7 system.
        1. Please name the file according to the following format:
            1. Customer-Site-V7-Server-MMDDYY-Field.ARQ
            2. Example: XYZCompany-Chicago-V7-Server-031214-Field.ARQ

Roll Back Procedure

> Should you encounter a fatal issue that requires the new version to be removed and revert to the previous revision, follow this procedure.
>
> Note that ARQ files are not typically backwards compatible. Therefore, ensure you use an ARQ generated with the appropriate revision of Foreseer.

1. Stop the Eaton Outpost Service. The Eaton Foreseer Apache Service should stop once the Foreseer service has stopped.

2. Run ServiceSetup.exe located in the Foreseer path. Uninstall both the Eaton Outpost and Eaton Foreseer Apache services. Verify that Administrative Tools>Services no longer contains an entry for either service. A reboot may be necessary.

3. Go to Control Panel>Programs and Features. Find Eaton Outpost and select Uninstall.

4. After the uninstall process has completed, remnant configuration files may be present in the directory where it resided. These files should be deleted or moved to an alternate location to prevent confusion.

5. For Option 1 installation scenarios:
    5.1. Run Outpost.exe from the installation directory where v6.3.172 resides. Verify that all devices are communicating. Verify general functionality and run a Log Report if necessary.
    5.2. Run ServiceSetup.exe and install the Eaton Foreseer service. Start the service in Administrative Tools>Services.
    5.3. Verify general WebViews and WebConfig functionality.

6. For Option 2 installation scenarios:
    6.1. Install Outpost/PXbridge v6.3.172 and follow the installation wizard steps.
    6.2. Start Outpost.exe and restore your archived v6.3.172 ARQ.
    6.3. Once the ARQ has been restored, verify general functionality and run a Log Report if necessary.
    6.4. Run ServiceSetup.exe and install the Eaton PXbridge/Outpost service. Start the service in Administrative Tools>Services.
    6.5. Verify general WebViews and WebConfig functionality.

Configuration Checklist

The following page contains a configuration checklist for yourForeseer installation. Print this page and complete the checklist before starting configuration.

Configuration Checklist

			Serial Settings					
Device Number	**Device Name**	**Network Settings IP Address**	**Serial Port**	**Baud Rate**	**Parity**	**Data Bits**	**Stop Bits**	**Flow Control**
1	UPS #2	189.100.150.22	N/A	N/A	N/A	N/A	N/A	N/A
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								

Copyright

Installation and Upgrade Guide – 7.9.200

Publication date 02/2025