BigFix Resolve Admin Guide

Special Notice

Before using this information and the product it supports, read the information in the Notices section at the end of this document.

Edition Notice

This edition applies to BigFix Resolve Admin Guide version 1.1 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Table of Figures

List of Tables

1 Introduction

In today's digital workplace, peak employee performance is imperative which can be hard to achieve. With the proliferation of devices, applications, and data, today's stretched IT staff needs to reduce help desk incidents while increasing user satisfaction. HCL BigFix Resolve is a User Workplace Optimization Solution that leverages the power of BigFix to enable user self -help to initiate essential fixes without the need for IT intervention. Unlike solutions that only recommend actions, BigFix Resolve enables users to remediate issues in real-time.

HCL BigFix Resolve is a user workspace optimization solution that leverages the power of BigFix to enhance the employee digital experience. BigFix Resolve minimizes IT Support burdens by pre-emptively resolving commonly occurring system or application issues through unassisted automation, using its powerful "Sense Heal" technology. By simplifying the use of BigFix content at the endpoint, BigFix Resolve helps end users solve their own problems, increasing productivity and lowering operational costs. For the first time, end users can leverage advanced BigFix automation with a single click. In contrast to solutions that require extensive set-up and custom rule creation, BigFix Resolve leverages predefined automations to optimize the user's digital experience.

2 Elements of BigFix Resolve

BigFix Resolve comprises the following elements –

1. Fixlets (approximately 60 scripts):
   - Self-healing
   - One-Click Solutions

Self-Healing Fixlets are pre-built remediation tasks that can be customized to meet the specific needs of an organization. These fixlets are designed to automatically remediate known issues on endpoints, such as patching software or updating drivers. Self-Healing Fixlets can run automatically, and they can be scheduled to run at specific times or triggered by specific events.

One-Click Solutions, on the other hand, are designed to provide a quick and easy way to remediate issues on endpoints. These fixlets are typically used for common tasks such as installing software, changing configurations, or restarting services. One-Click Solutions can be run with a single click by end-users or IT staff, and they are designed to be simple and easy to use.

Self-healing fixlets can be configured as policy actions and one-click fixlets can be configured as offer actions.

Figure 1 - Self-Healing Fixlets/One-Click Solutions

Fixlets in the One-Click Solutions/Self-Healing category can be configured as a Policy (Self-Healing) or One-Click (Offer) action, whereas fixlets that do not contain the Self-Healing category can only be configured as a One-Click (Offer) action.

2. Components:
   - BigFix Resolve WebApp
   - BigFix Resolve Client Dashboard

   This dashboard consists of two Self Service tabs:
   - Assistant
   - Ticket

2.1 BigFix Resolve WebApp

This is a web service built on **IIS (Internet Information Services)** that is used for Service Now integration (an optional component, anyone can opt in or opt out of it), allowing end users to use the BigFix SSA Ticket Dashboard to raise a ticket for fixes that are not available in the catalog.

System requirements for the **BigFix Resolve WebApp** are as follows:

2.1.1 Hardware requirements

The requirements are for a server where BigFix Resolve Webapp needs to be installed in case Service Now integration feature is used.

Table 1 - System requirements for BigFix Resolve WebApp

Requirement	Recommended	Minimum
CPU	4	2
Memory	8 GB	4 GB
Processor Architecture	32-bit processors 64-bit processors	32-bit processors 64-bit processors
Processor	2.3 GHZ	1.8 GHZ
Disk Size	20 GB Free Disk	20 GB Free Disk
Operating System	Window Server 2016 & above	Window Server 2016 & above

2.1.2 Software requirements

IIS Version: 10.0

Manually install IIS on the server where you want the BigFix Resolve Webapp to be installed.

IIS (Internet Information Services) is a web server software developed by Microsoft for hosting and serving web applications and websites on Windows operating systems.

.NET Core: ASP.NET Core Runtime 8.0 or higher

This will be deployed automatically by the Resolve Webapp Fixlet

2.1.3 Certification requirement

SSL Certificate:

A trusted SSL certificate issued by a recognized Certificate Authority (CA)

This certificate is mandatory, and the configuration cannot be completed if it is not provided. The customer has to obtain the certificate themselves. Currently, only trusted CA certificates are supported by SSA.

Using the SSL Certificate involves the following steps:

This is only applicable if BigFix Resolve Webapp is successfully installed. For installation, please refer to section 2.1.6.

1. Login to BigFix Resolve Server and go to Search to look for IIS (Internet Information Services)

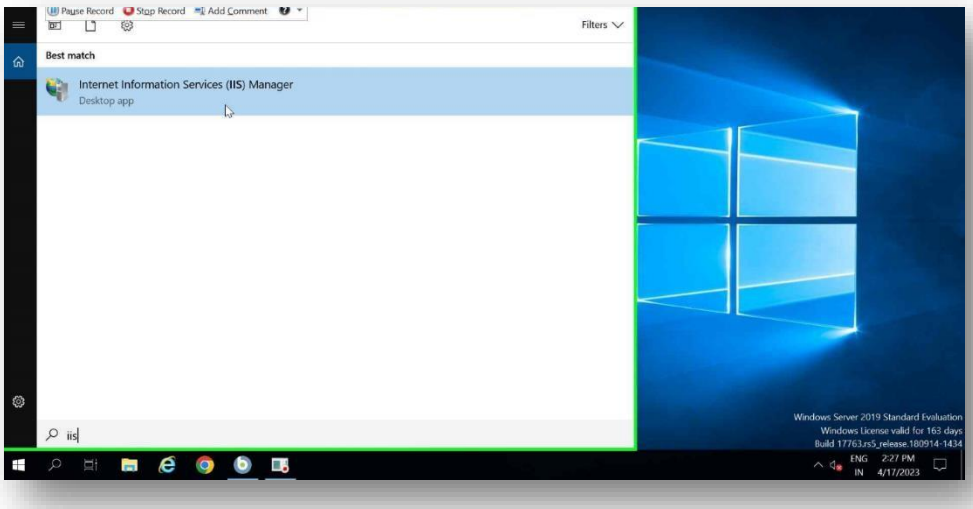

Figure 2 - BigFix Resolve Server

2. Run it as Administrator

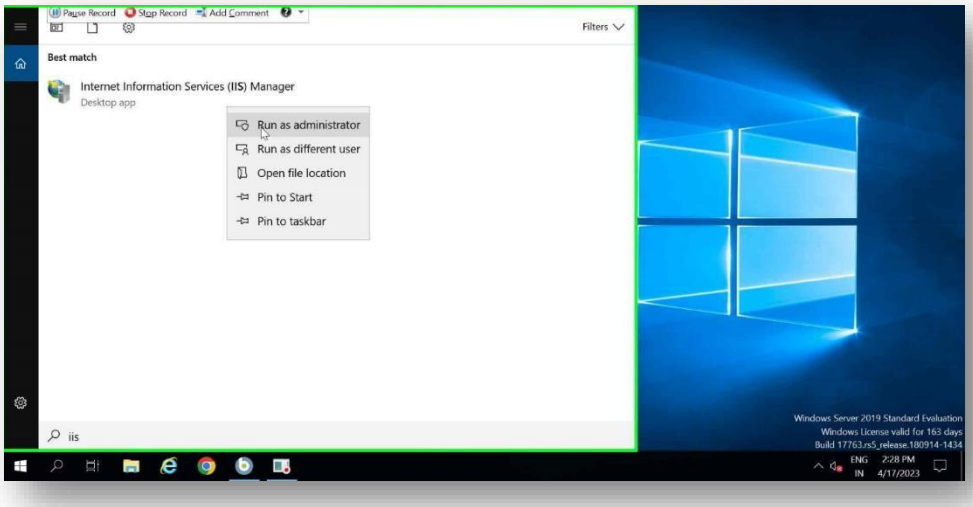

Figure 3 - Run it as Administrator

3. Check if the BigFix Resolve Site exists

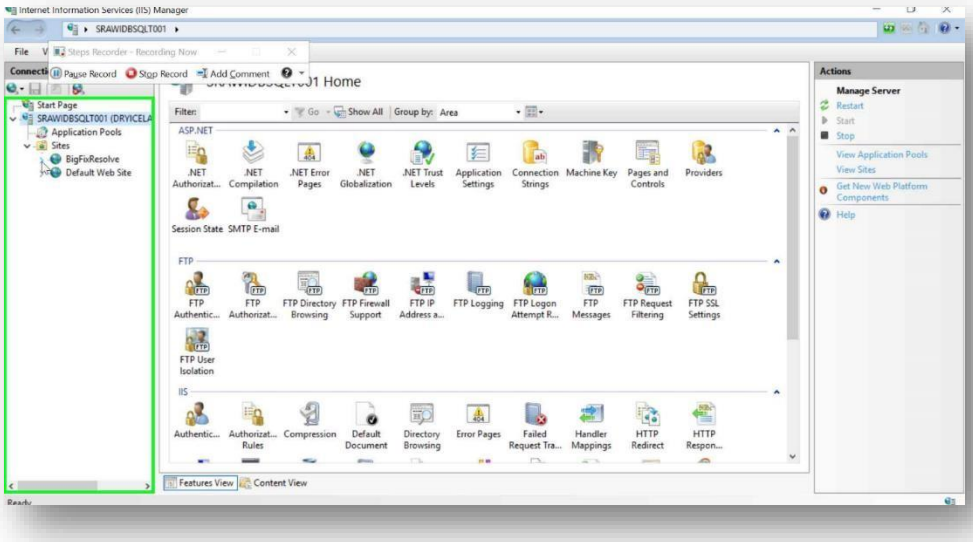

Figure 4 - BigFix Resolve Site

4. Right click on BigFix Resolve Site. Then click on Edit Bindings and check for HTTPS Certificate

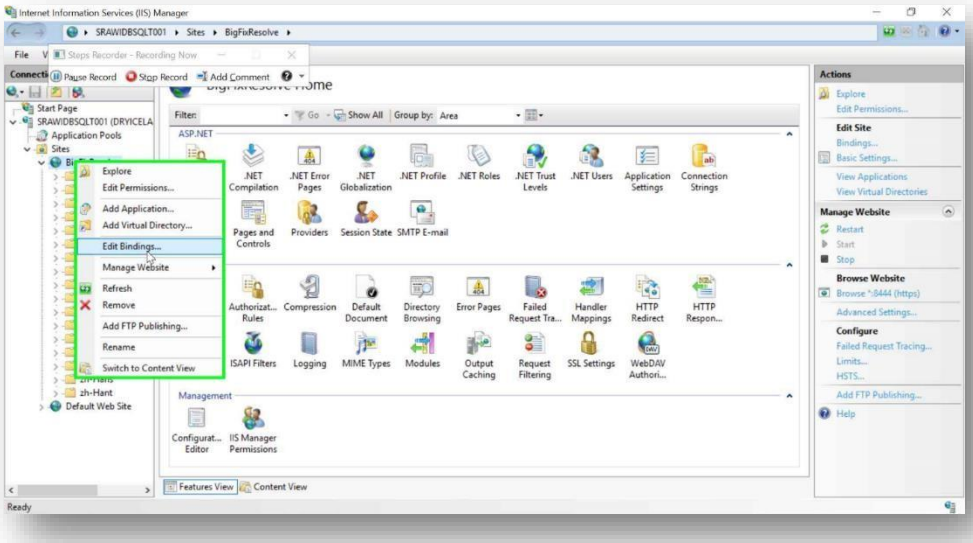

Figure 5 - Edit Bindings

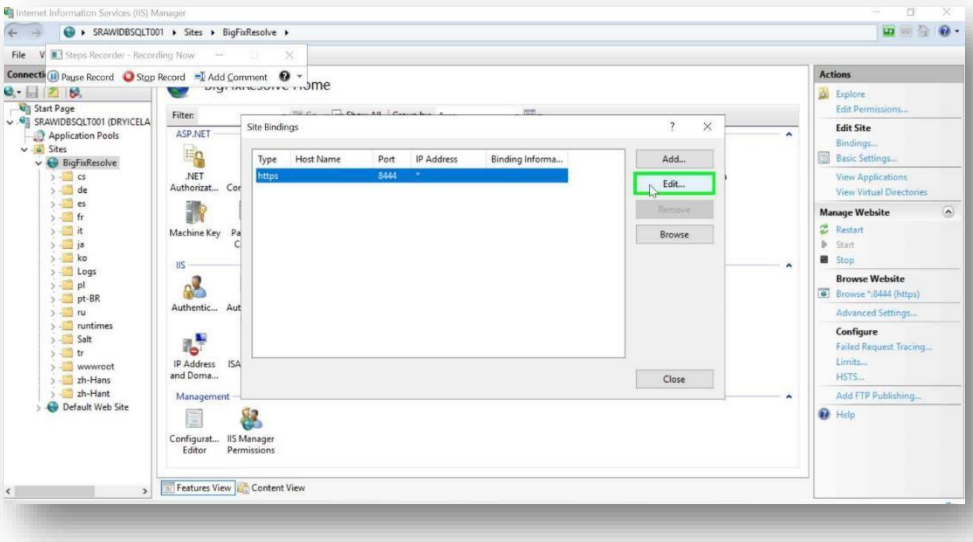

Figure 6 - Edit

5. By default, it will show a CA-signed Certificate but we require a host-based certificate. So, click on Cancel.

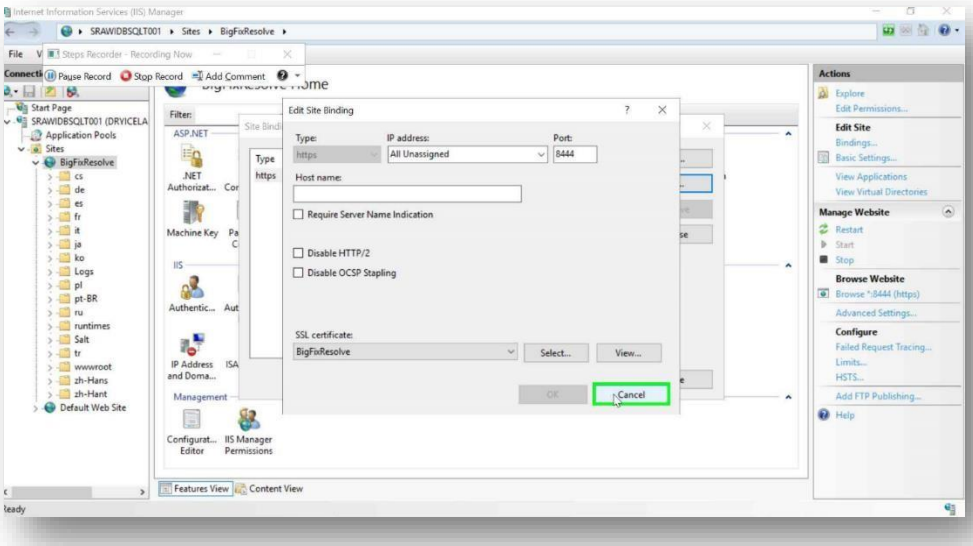

Figure 7 - Cancel

6. Then click on Close, to close the dialoge box

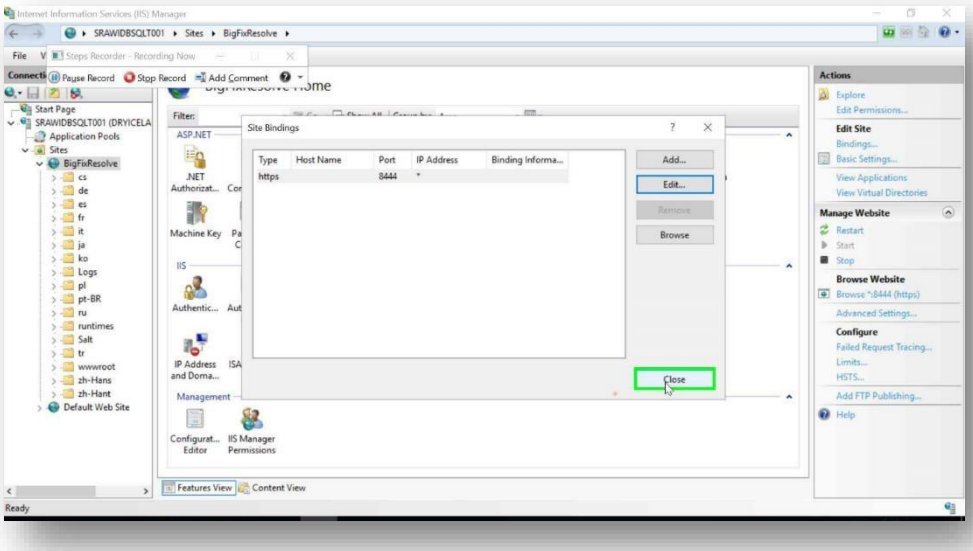

Figure 8 - Close

7. For Host-based certificate, go to the path where Host-based certificate is downloaded

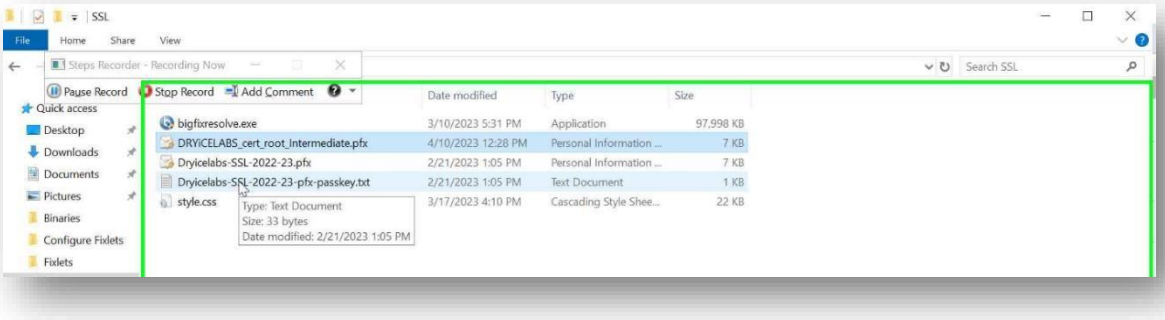

Figure 9 - Host-based certificate

8. Copy the password of the Certificate

Figure 10 – Copy Password

9. From the same path, right click on the Certificate file, and click on Install PFX to install it

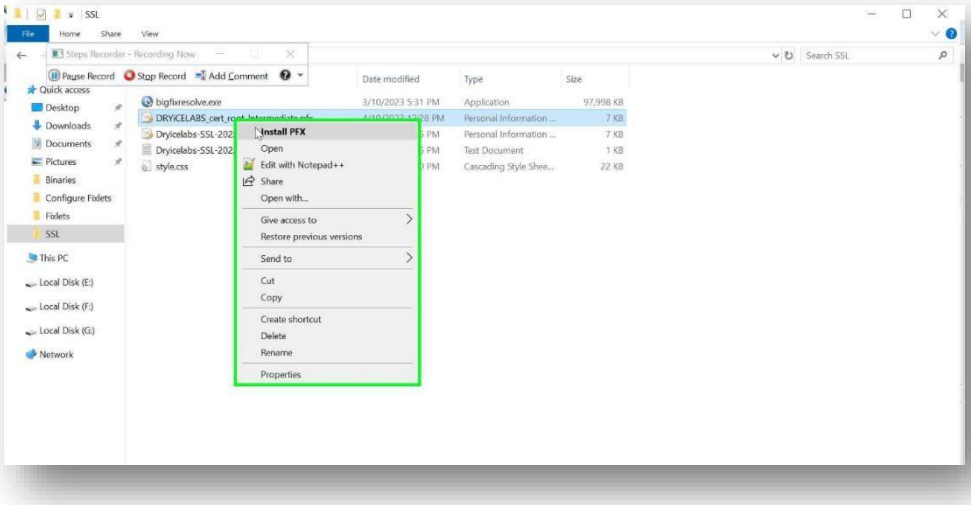

Figure 11 - Install PFX

10. Select Local Machine and click on Next.

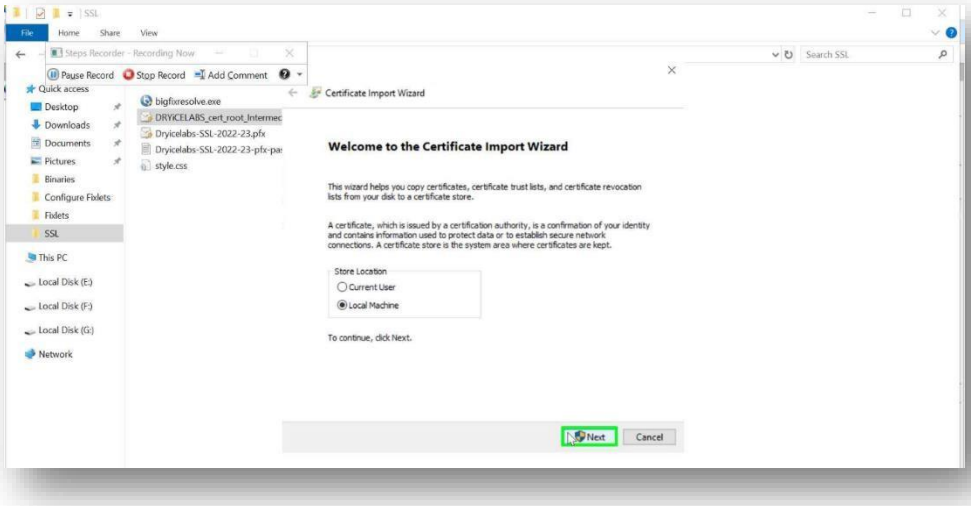

Figure 12 – Next

11. In the next page shown, click on Next.

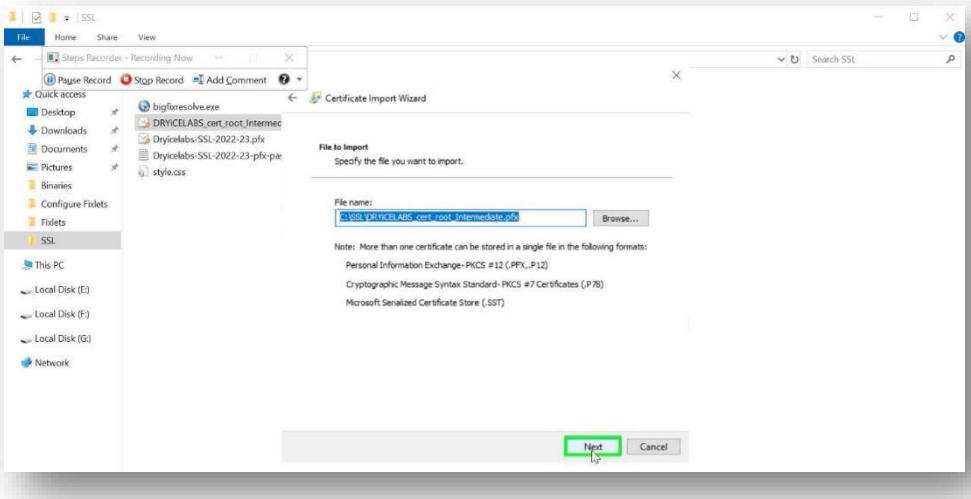

Figure 13 - Next

12. Paste the password copied in the previous step and click on the following action buttons until the import is successfully finished

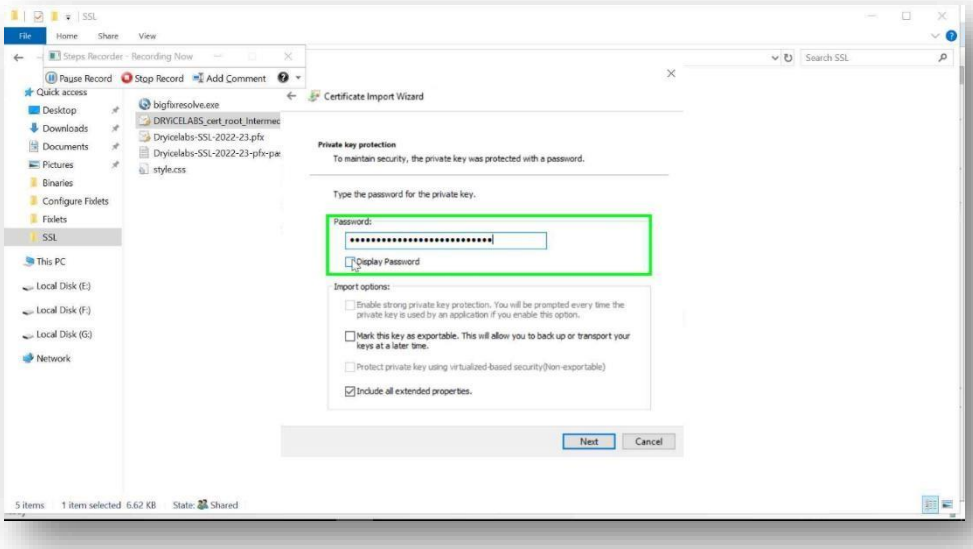

Figure 14 – Password pasted

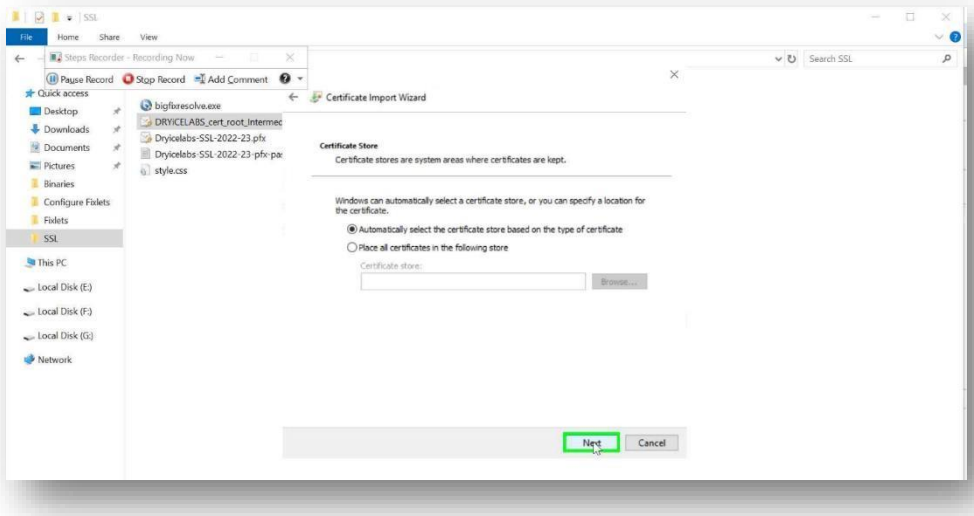

Figure 15 - Next

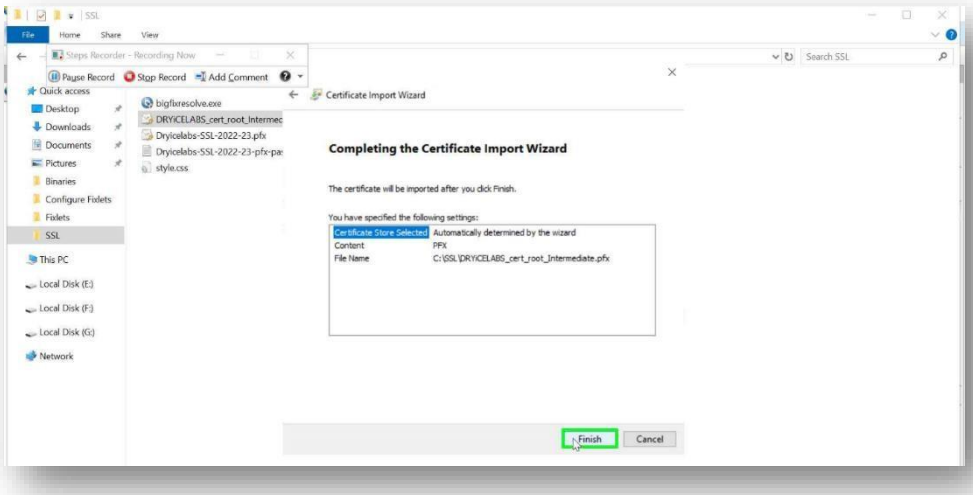

Figure 16 – Finish

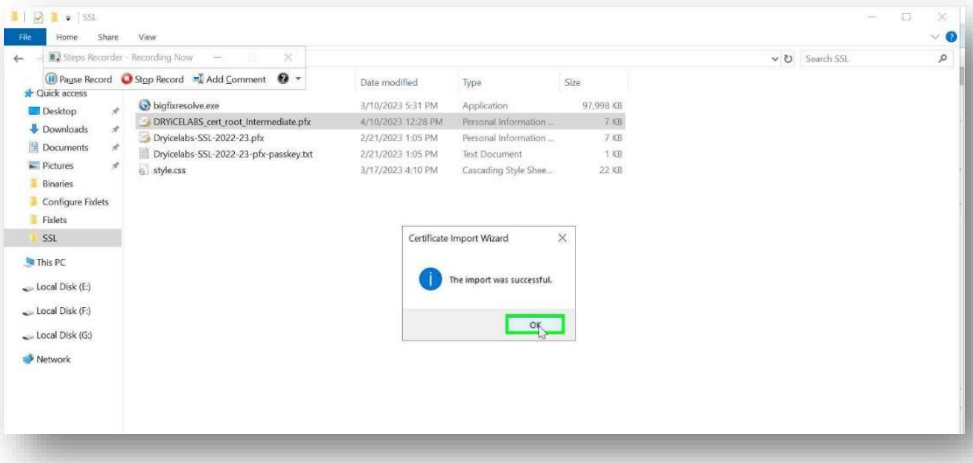

Figure 17 - Ok

13. Go to Search, type MMC and run it as administrator to check if the certificate is installed properly

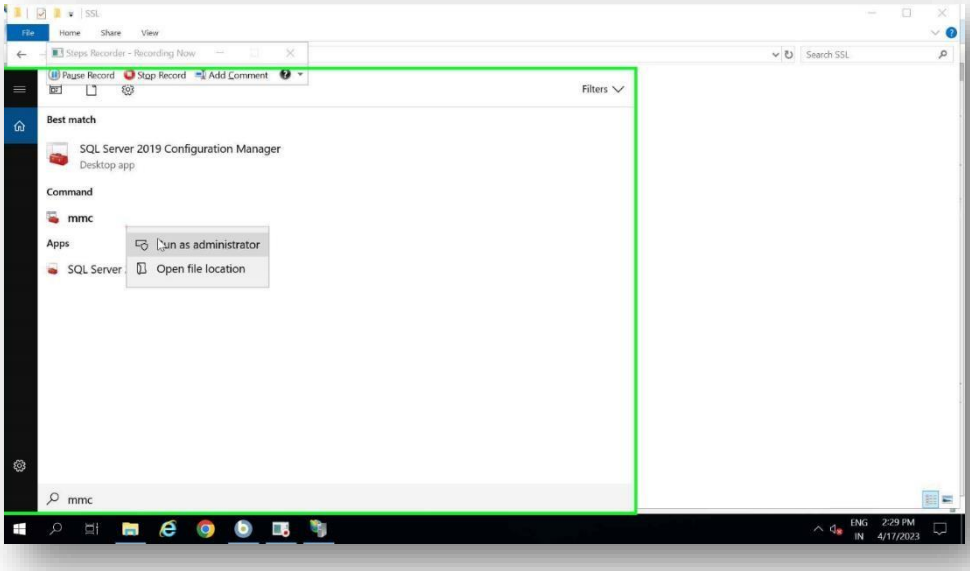

Figure 18 – Run as administratitor

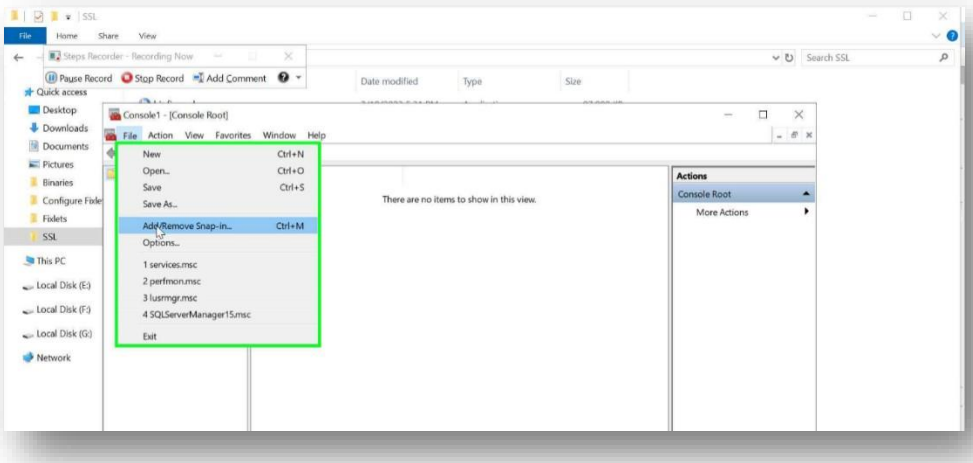

Figure 19 – Add/Remove snap in

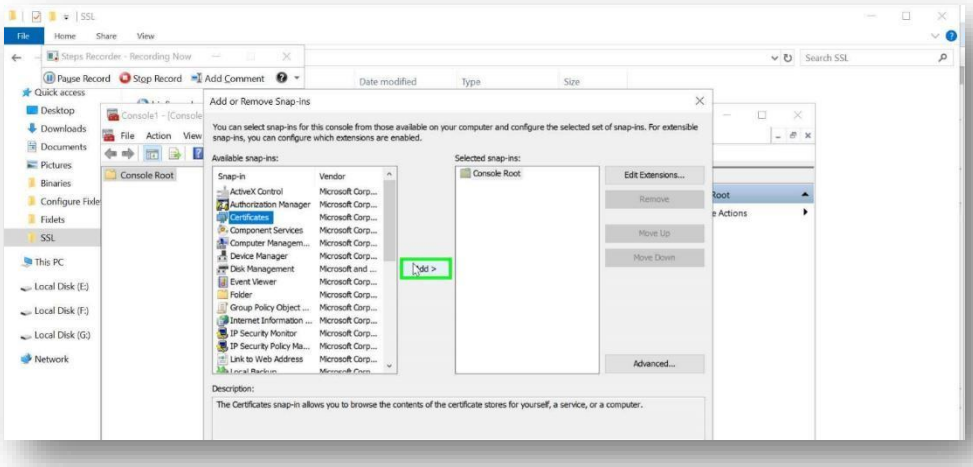

Figure 20 – Add

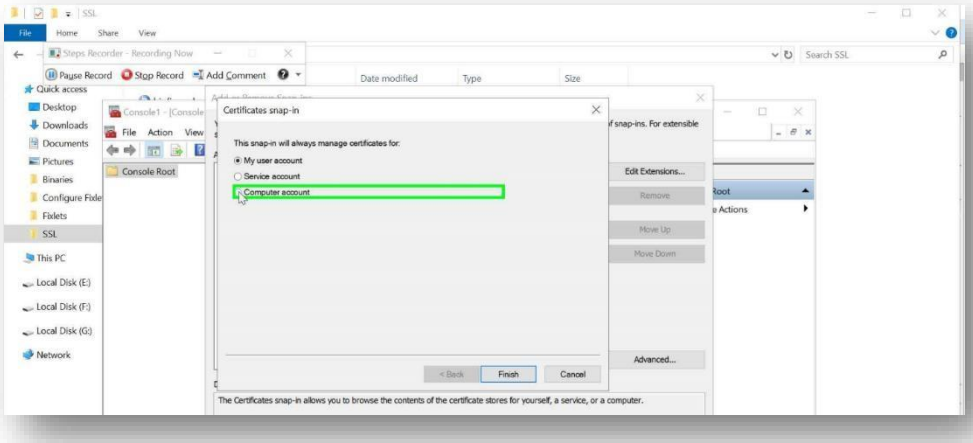

Figure 21 – Computer account

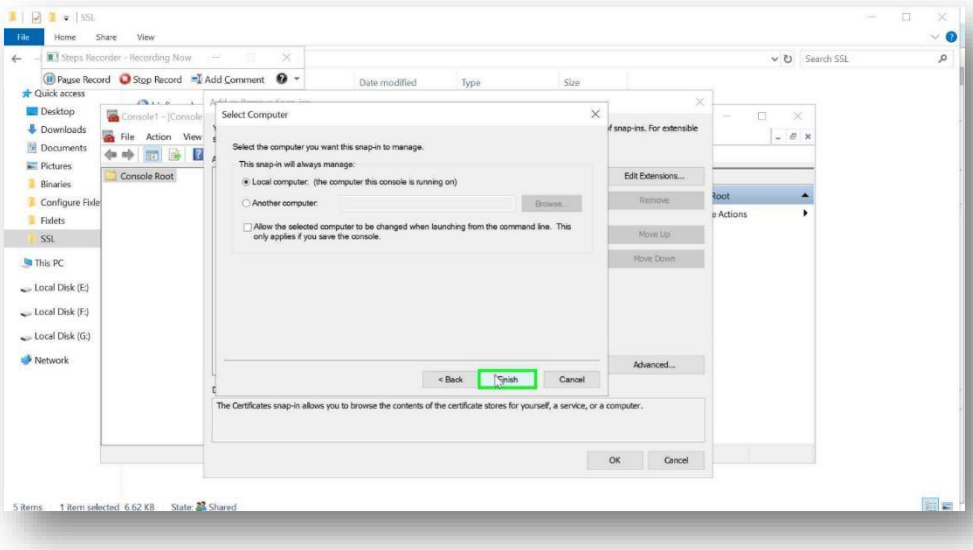

Figure 22 - Finish

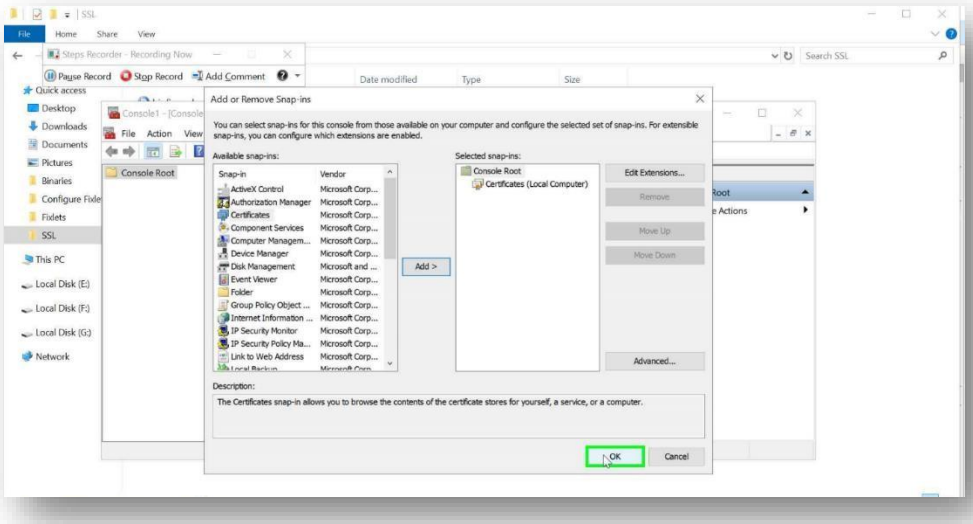

Figure 23 - Ok

14. Now under Certificates, go to Personal and click on Certificates. The installed certificates will be shown on the right hand side

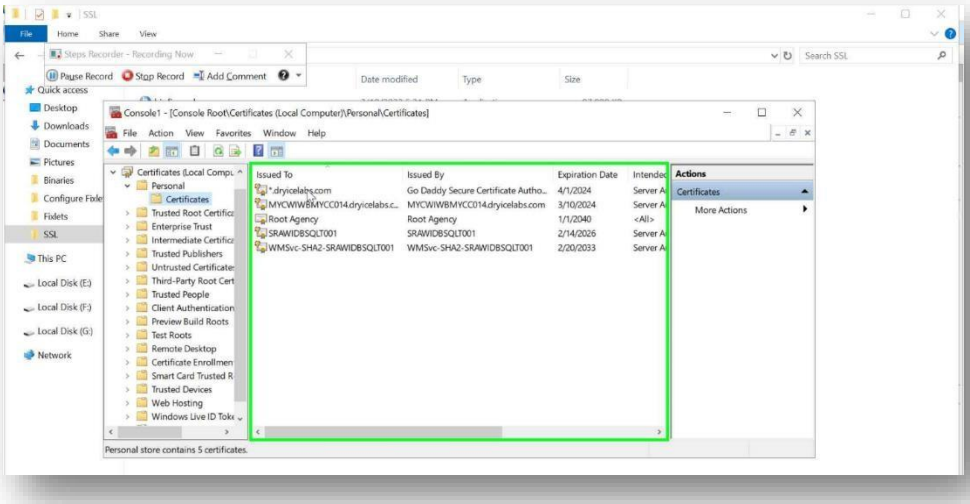

Figure 24 - Certificates

15. Go to Search, type IIS and run it as administrator. Under Sites, right click on the BigFixResolve site and select Edit Bindings

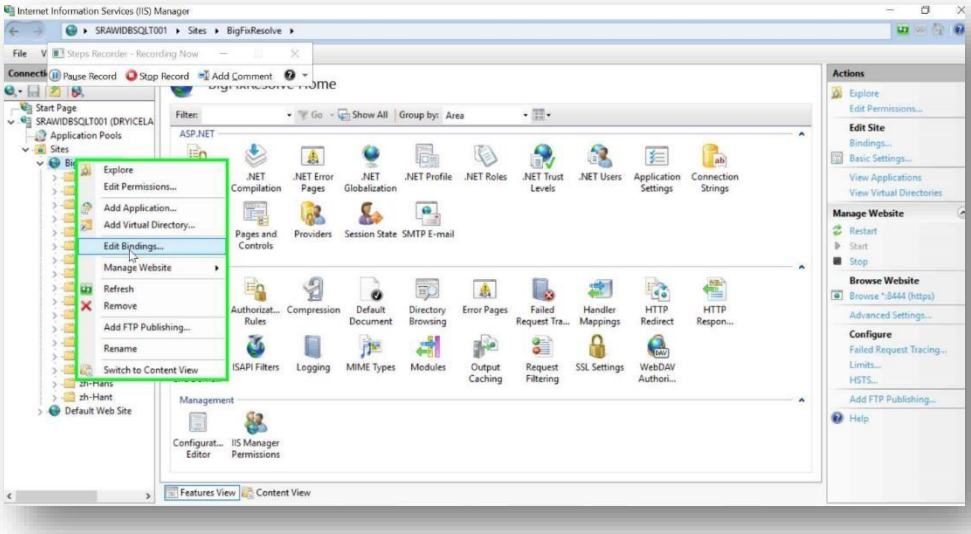

Figure 25 - Edit Bindings

16. Click on HTTPS Edit and select the installed certificate instead of default CA signed certificate

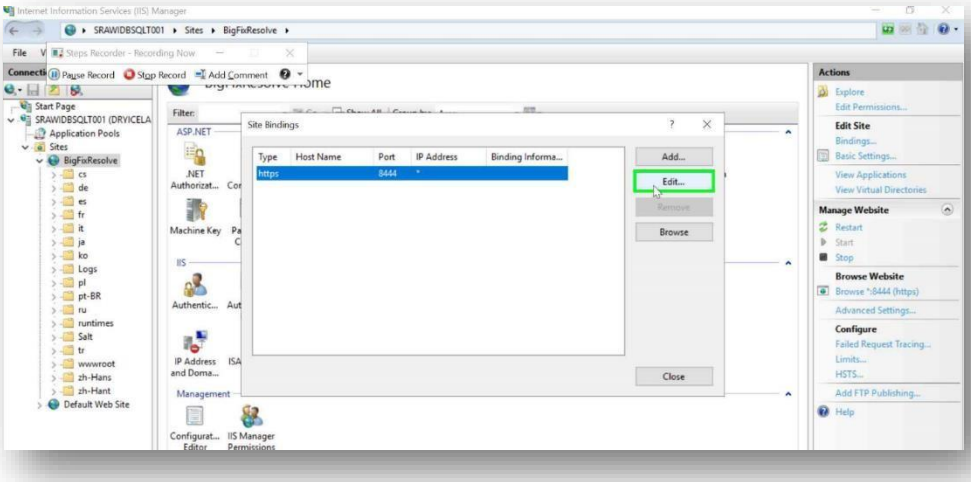

Figure 26 - Edit

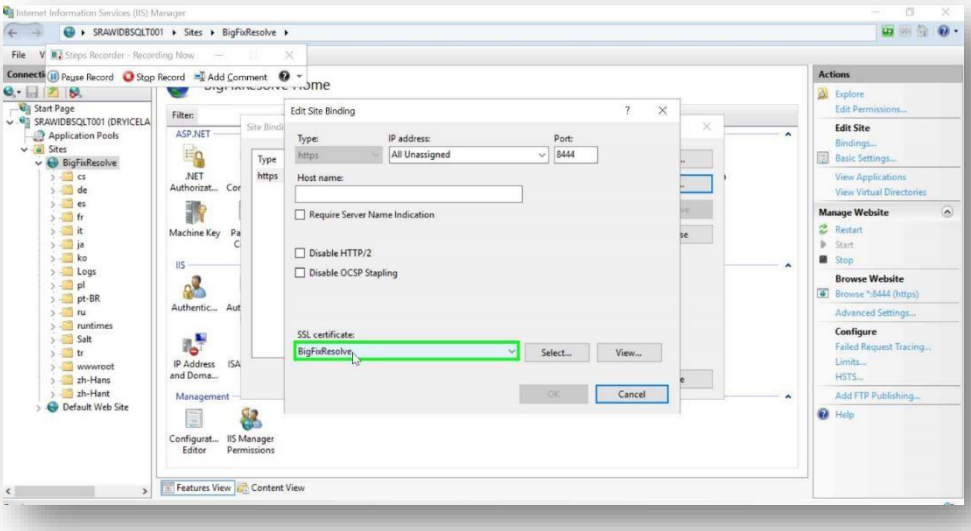

Figure 27 – SSL Certificate

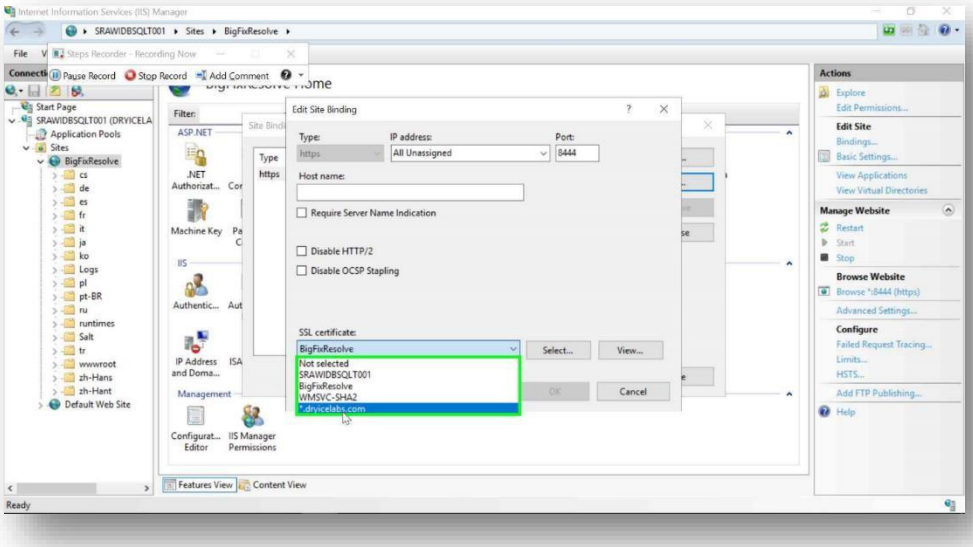

Figure 28 - SSL Certificate

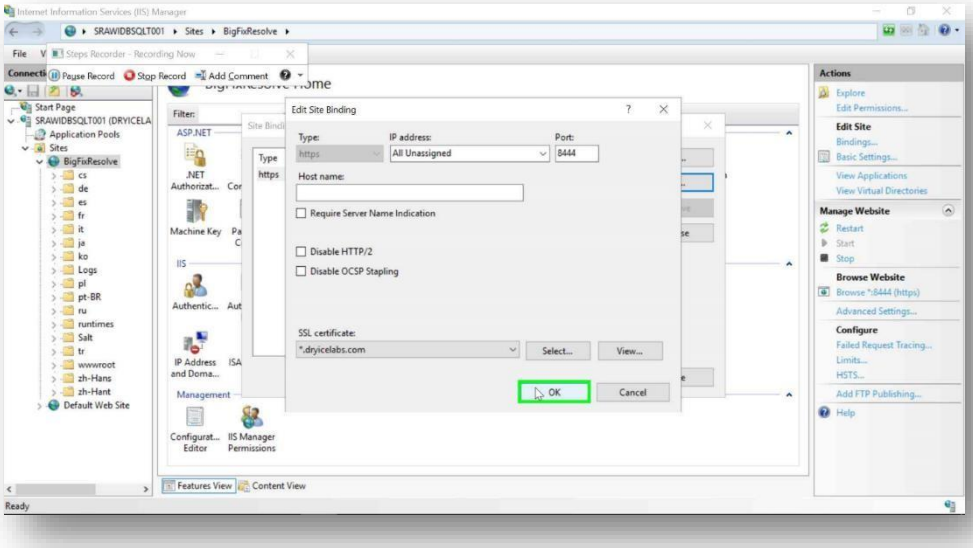

Figure 29 - OK

17. Restart the Website

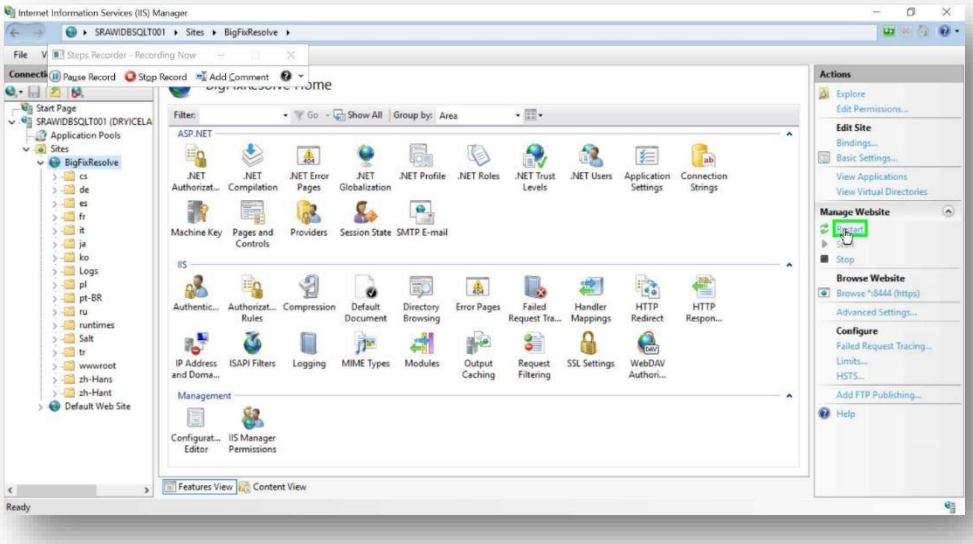

Figure 30 – Restart website

18. To check for the hostname, open the command prompt and copy it

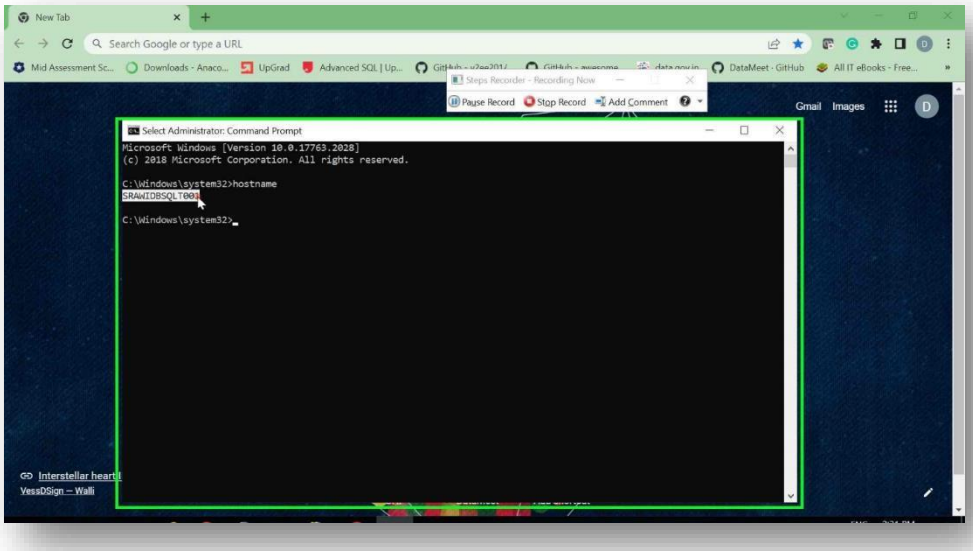

Figure 31 – Copy hostname

19. Next, open the Browser (Chrome) and enter the FQDN

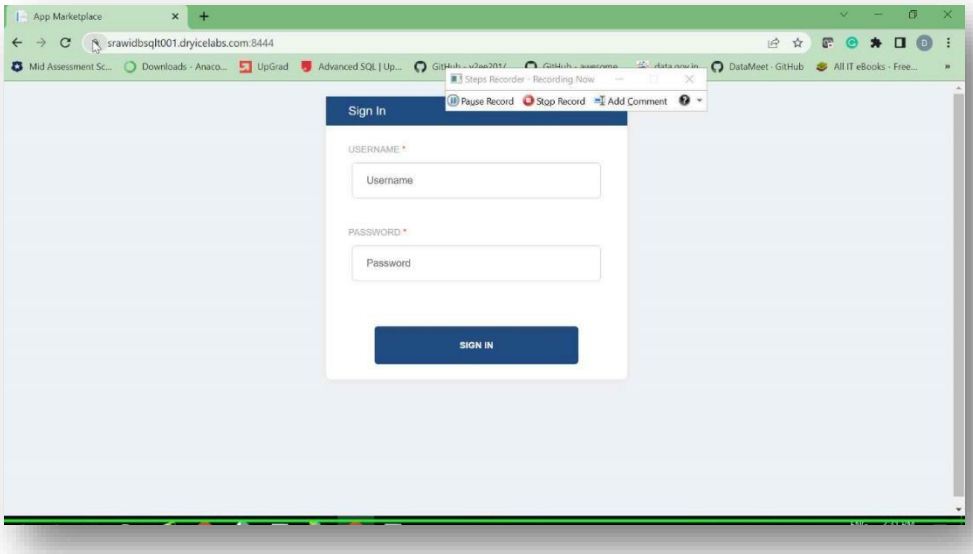

Figure 32 - FQDN

20. Check for Certificate, you will find “Certificate is Valid” shown there

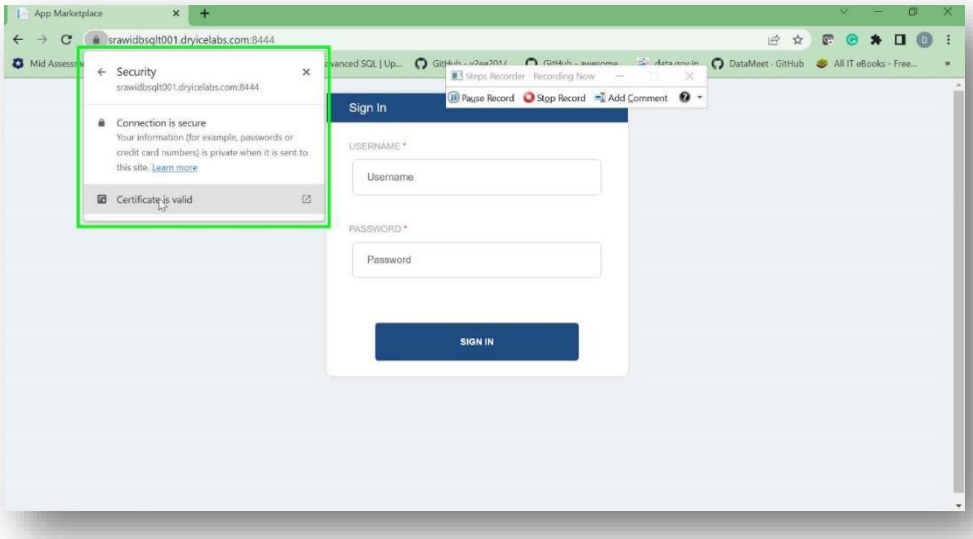

Figure 33 - Certificate is Valid

This concludes BigFix Resolve HTTPS Certificate installation.

2.1.4 Integration requirement

BigFix Resolve Web App integrates with Service Now, which requires Service now OAuth 2.0 Service now credentials and the organization's LDAP URL.

2.1.4.1 Service Now

Service Now is a cloud-based platform that provides IT service management, IT operations management, and business management services. It also provides an API for developers to integrate with other systems. This section explains how to use OAuth 2.0 authentication to integrate ServiceNow with another system.

OAuth 2.0 Credentials are required for integrating BigFix Resolve and Service Now.

OAuth 2.0 is a standard protocol used for authorization and authentication.
It is widely used by web and mobile applications to access user data from other services without requiring users to provide their credentials to those applications.
To set up OAuth2.0 and access OAuth Applications, please visit: https://docs.servicenow.com . For further details, please connect to the Service Now admin at your organization to setup Service Now Oauth2.0.

The pre-requirements for Service Now are:

- Base URL: This is the ServiceNow instance URL, which is used to access the ServiceNow application.
- Username: This is the username of the account that will be used to authenticate and access the ServiceNow instance.
- Password: This is the password for the above-mentioned username.
- Client ID: This is a unique identifier for the client application that is integrating with the ServiceNow instance.
- Client Secret: This is a confidential secret that is used to authenticate the client application with the ServiceNow instance.

- Contact Type: This field specifies the type of contact that is created when a new incident is logged in ServiceNow. The default value is email, but it can be set to other options depending on the organization's requirements.
- Short Description: This field specifies the short description of the incident that is created in ServiceNow. The default value is "Resolve", but it can be set to other options based on the organization's requirements.
- Assignment Group: This field specifies the group that will be responsible for handling the incident.
- Assignment Group Get: This field specifies the group that will be used to look up the incident assignee.

Service Now Service Account should have access to REST API to Create and Update Incidents.

2.1.4.2 LDAP: Company's LDAP URL (PATH) and Domain Name

BigFix resolve WebApp integrates with LDAP for Service Now integration as it adds a layer of authentication that only the authorized users can access.

LDAP (Lightweight Directory Access Protocol) is a protocol used for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. A company's LDAP URL is the web address or hostname of their LDAP server, which allows users to connect to and access the company's directory services. This URL is used to authenticate users and provide access to various resources within the company's network, such as email, files, and applications. The LDAP URL typically begins with the prefix "ldap://" or "ldaps://" for secure connections, followed by the hostname or IP address of the server and the port number. ldap://ldap.example.com or ldaps://ldap.example.com

In this example, "ldap://" indicates that the protocol being used is LDAP, "ldap.example.com" is the hostname of the LDAP server, and ":389" is the port number where the server is listening for LDAP requests. The port number 389 is the default port used for LDAP communication, but it can be different depending on the configuration of the LDAP server.

2.1.5 Firewall requirement

Firewall and Ports requirements:

Table 2 – Firewall Requirements

S.No	Source	Destination	Port	Protocol
1	All BigFix clients that have SSA and the BigFix Resolve Client Dashboard installed	BigFix Resolve Web App Server	8444*/ (ANY HTTPS PORT)	HTTPS
2	BigFix Resolve Web App Server	LDAP Server	389, 636	

HTTPS 443, Network Access to ServiceNow REST APIs

*BigFix Resolve WebApp can be configured to communicate on any https port, proper firewall rules must be in place to accept the communication to BigFix Clients/SSA.

2.1.6 Installing BigFix Resolve WebApp

To install the BigFix Resolve WebApp, BigFix V10.0.8.37 & above needs to be installed and BigFix Agent Running on the server where the BigFix WebApp needs to be installed. Before the user begins installing the Resolve WebApp, they need to ensure that their system fulfills all of the prerequisites. The BigFix Resolve WebApp can then be installed by running a Task from the BigFix interface.

Install the Resolve WebApp by completing the following steps:

1. Read the pre-requisite information before the installation.
2. Subscribe to BigFix Resolve Site from License Dashboard under BigFix Management Domain.
3. Run the Task that installs the BigFix Resolve WebApp from the External Site – BigFix Resolve. The installation takes a few minutes. The Task that installs the BigFix Resolve WebApp is no longer relevant once the installation is setup.

   Provide the following inputs:

   - LDAP URL
   - Domain Name
   - Base URL - Service Now URL: This is the ServiceNow instance URL, which is used to access the ServiceNow application.

- Username: This is the username of the account that will be used to authenticate and access the ServiceNow instance.
- Password: This is the password for the above-mentioned username.
- Client ID: This is a unique identifier for the client application that is integrating with the ServiceNow instance.
- Client Secret: This is a confidential secret that is used to authenticate the client application with the ServiceNow instance.
- Contact Type - Email (Default)/Optional: This field specifies the type of contact that is created when a new incident is logged in ServiceNow. The default value is email, but it can be set to other options depending on the organization's requirements.
- Short Description - Resolve(default)/ Can be set according to organization requirements: This field specifies the short description of the incident that is created in ServiceNow. The default value is "Resolve", but it can be set to other options based on the organization's requirements.
- Assignment Group: This field specifies the group that will be responsible for handling the incident.
- Assignment Group Get: This field specifies the group that will be used to look up the incident assignee.
- Port Number
- Drive location where Resolve Application will be Installed

4. Verify that BigFix Resolve WebApp was properly installed and is running. (Under Program and Features)
5. Launch a browser and type https://Hostnameofserver:port to verify if the site is accessible.

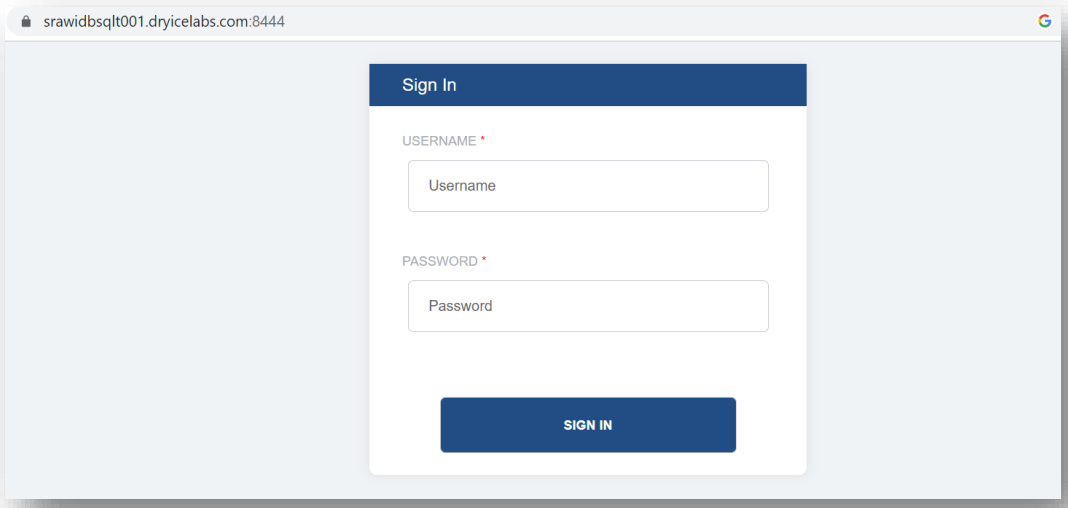

Figure 34 – Sign In

2.2 BigFix Resolve Client Dashboard

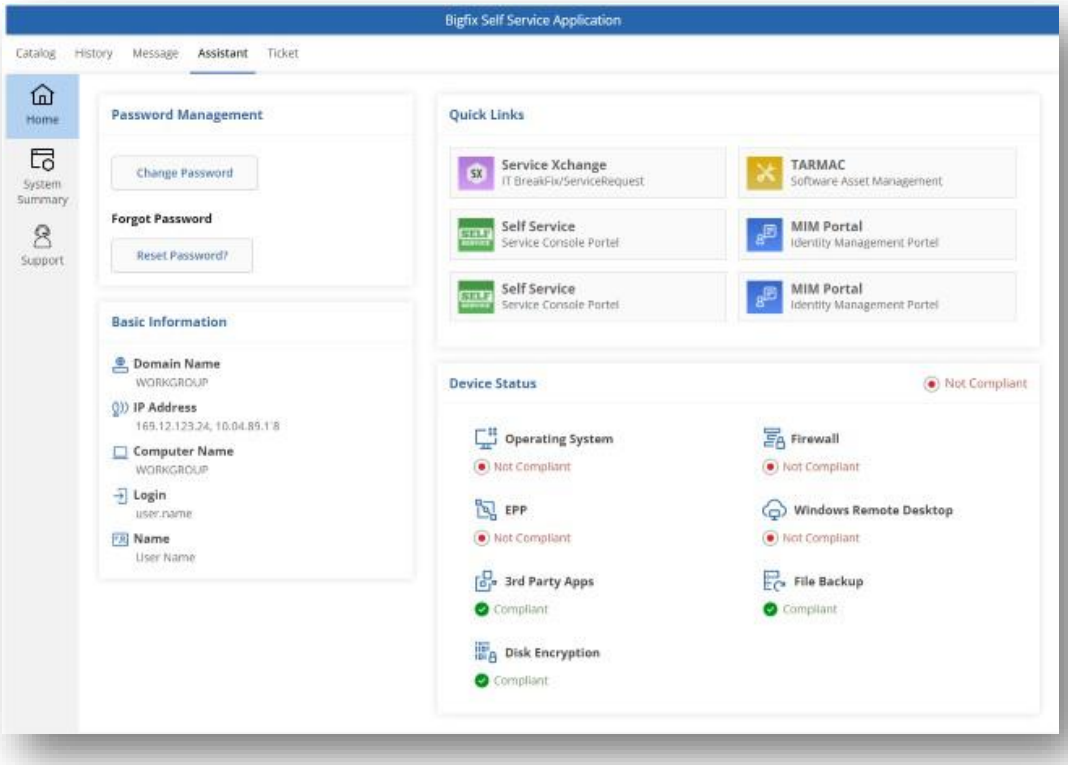

Figure 35 – Client Dashboard (Assistant)

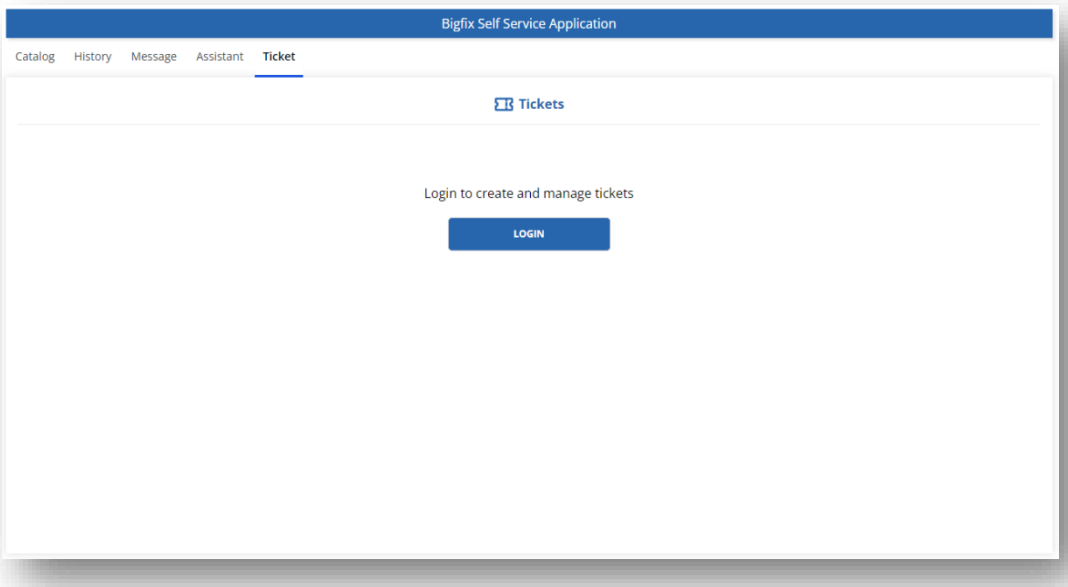

Figure 36 – Client Dashboard (Ticket)

BigFix Client Dashboard is an extension to BigFix Self Service Application that provide the Assistant and Ticket Dashboard to the end users.

Pre-requisites to installing BigFix Client Dashboard are:

- ***BigFix Self Service Application:*** SSA V2.2.4 & above installed on all the endpoints where you want BigFix Resolve Client Dashboard.

For requirements for BigFix Self Service Application refer to:

https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Self_Service_Application/SSA_Install_Config_Guide/c_sys_requs.html

Steps to install the BigFix Client Dashboard are as follows:

1. Verify that pre-req's for BigFix Resolve Client Dashboard Requirements are fulfilled.
2. Go to External Site — BigFix Resolve — Fixlets & Tasks — Run Install BigFix Resolve Assistance Task* on all the endpoints where SSA is installed.
3. Go to External Site — BigFix Resolve — Fixlets & Tasks — Run Install BigFix Resolve Assistance & Ticket Task on all the endpoints where SSA is installed.
4. Verify that the Assistant or Assistant & Ticket Tab are installed by accessing the Self Service Application.

*There are two tasks to install the BigFix Client Dashboard, depending on the organization 's requirements. If you have configured BigFix Resolve Web App for Service Now Integration, then please use Install BigFix Resolve Client Dashboard (Assistant)

2.2.1 Assistant

Assistant provides the user with a unified dashboard for device compliance, the organization's important links, basic information, and the password management section.

This section is visible to the end users only if enabled and configured by the BigFix Administrator who has access to the BigFix Resolve site.

- **Self-Compliance Check Panel**

  Provides the end user with immediate visibility into the endpoint's compliance status via a configurable pre-defined list of indicators.

- **Quick Links**

  Customizable Quick Links for easy access to knowledge base sites, resources, and documentations.

- **Password Management**

  Provides direct access to Organization's web pages for changing the password or reset in case it was forgotten.

- **System Summary**

  Provides a snapshot of the entire system's Hardware, Network, and Operating System properties.

- **Support**

  A unified dashboard for end users so that they can connect to e-mail, chat or call*.

*Phone number is only an indicator.

2.2.1.1 Configure Password Management Widget

A password management dashboard is a tool that helps users and administrators manage passwords and other credentials. It provides a centralized location for viewing and managing passwords, resetting forgotten passwords, and changing passwords as needed. They can improve security and simplify password management for users. To configure the Password Management Widget:

1. Go to External Site – BigFix Resolve – Use Configure BigFix Resolve Password Management Widget Task.
2. Enter the Change Password and Reset Password URL's and run the task on all the endpoints where SSA Assistant Tab is Installed.

After a successful configuration, if an end user clicks on change password and reset password they will be redirected to the URL set by the administrator.

Change password and reset password is not limited to only domain or any specific application and password link can be embedded by the admin which the organization wanted in there reset system.

2.2.1.2 Configure Quick Links

1. Go to External Site – BigFix Resolve – Use Configure Quick Link Widget Task.
2. Enter the Link Title, Description and URL, you can only add up to six quick links and run the task on all the endpoints where Assistant tab is Installed.

2.2.1.2.1 Adding Image to Quick Links

This section will help you change BigFix Quick Link Icons. To do so, we can utilize BigFix WebUi Send a File Feature.

For Details Please refer - Send a File (hcltechsw.com)

2.2.1.2.2 Upload files

This section explains you how to upload an image, send a file to target devices, and delete a file from the list.

Before you begin:

- The operator must have the following permissions:
  - Can Create Actions
  - Custom Content
- SWD must be running, and the operator must have access to it

To upload a new file into the server:

1. From the **Devices** page, select one or more devices.
2. Click **Configuration** and select **Send** file.

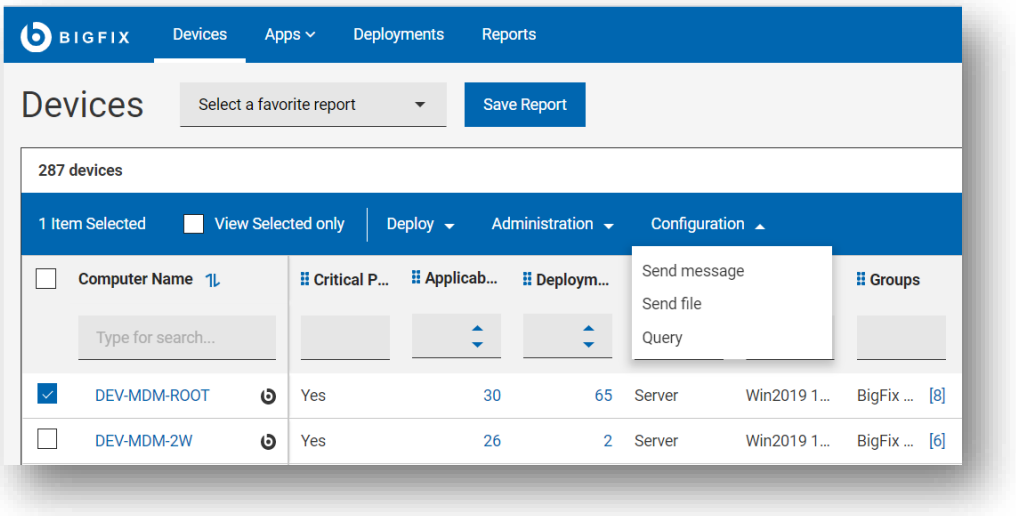

Figure 37 – Devices Page

The Files page is displayed that lists all the files which are already uploaded by the user.

3. Click **Upload**, navigate and select the file you want to upload (in our case it's icon for Quick Links), and then click **Open**.
4. The file uploading starts and you can see the status of the upload in the progress bar.
5. If you want to cancel the upload, click the red 'x' icon next to the progress bar.

Once the file is uploaded, the file list is updated, and the uploaded file becomes available to be sent on target devices.

If you are using Microsoft Edge browser to upload a file, ensure you are using the MS Edge version 18.18218 or later. With earlier versions of Microsoft Edge, the progress bar does not show the file upload status; however, the file list gets updated with the uploaded file.

2.2.1.2.3 Recommendations for uploading Quick Link Icons

- Image Dimensions - 44 * 41
- Width - 44 pixels
- Height - 41 pixels

While uploading any file for Quick Links, ensure that the File name is exactly the same as given in Quick Links

E.g., MIM Portal.jpg (Refer Below)

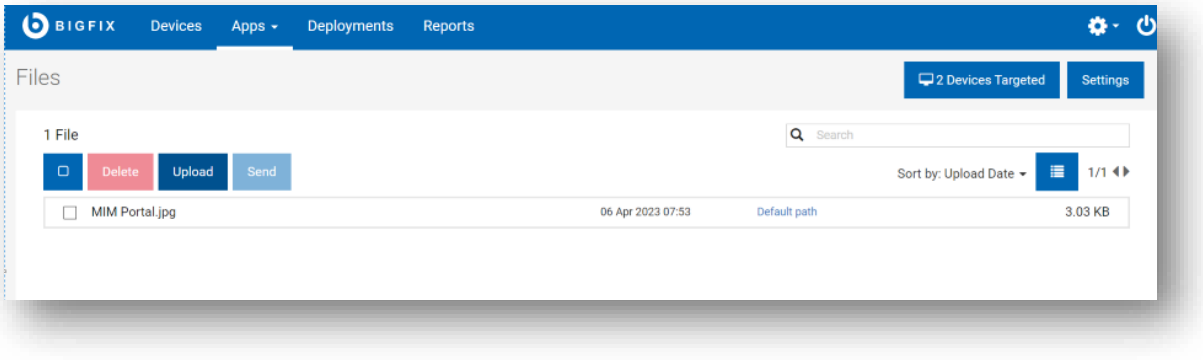

Figure 38 – File Name

When the file is uploaded, it is saved in the default path. To change the default path:

a. Click the link **DEFAULT_PATH** against the file for which you want to change the default path.

b. In the **Destination file path** window: (Directory location of BigFix Client):\Program Files (x86)\BigFix Enterprise\BES Client__BESData__UISupport\Assistant

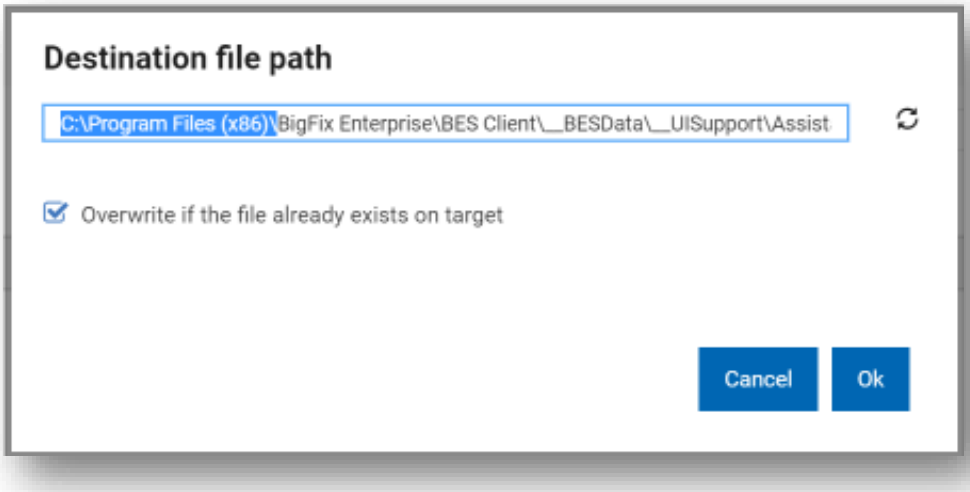

Figure 39 – Destination File Path

c. Enter the desired path.

d. Select the option Overwrite if the file already exists on target if necessary.

e. Click **Ok**.

The specified path is set as the destination path.

2.2.1.2.4 Send a file

You can select a file and send it to one or more selected devices.

Prerequisites:

The user permission required to send a file are **Create Action** and **Custom Create**.

To send a file to one or more destination devices:

1. In the Devices page, go to the list of devices, and select one or more destination devices to which you want to send a file.

Important:

Select at least one destination device.
If you want to select more than one device, then select devices that belong to the same operating system.

2. Click More and select Send file.
3. From the list of files, select a file to transfer.

Important: You can send only one file at a time.

You can search and find a file, and sort by upload date, file name, or file size.

- **Devices Targeted –** This displays the number of devices selected. Click this button if you want to modify your device selection**.**
- **Settings –** Click this button to define file transfer settings**.**

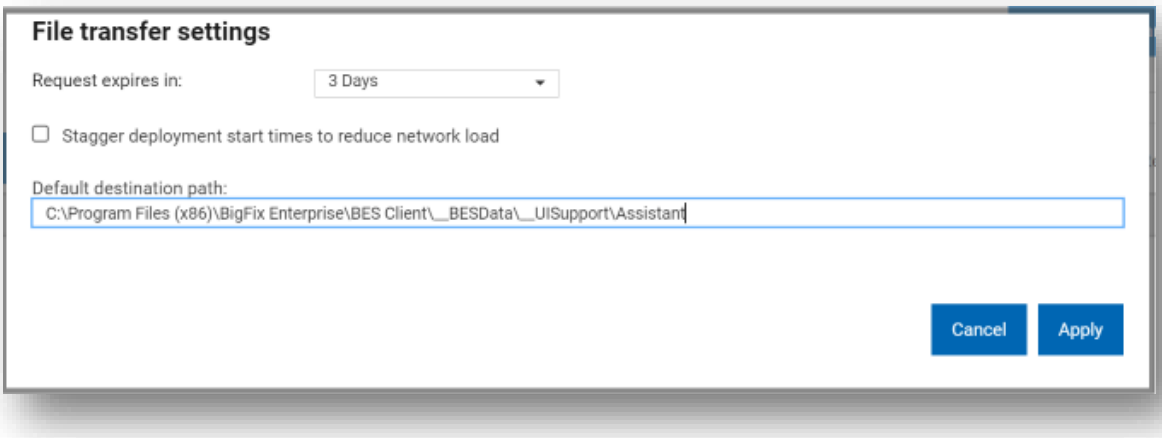

Figure 40 – File Transfer Settings

- **Request expires in –** Select a time period from the drop-down list within which the file can be transferred to the destination devices. After this time period, the file transfer request expires and the file cannot be transferred.
- **Stagger deployment start times to reduce network load** – Select this option if you want to reduce network load.
- **Default destination path –** Specify the default destination path where you want to transfer the file in all selected devices.

4. Click **Send**.

After successful transfer, the file becomes available in the destination devices at the default path set.

2.2.1.2.5 Delete

To delete files from the server, from the list of files, select one or more files and click Delete.

If you want to use only few Quick Links, then Keep the remaining blank.

2.2.1.3 Configure Device Status Widget

Device Status gives the end-user the option to monitor device compliance status by themselves.

- **Operating System**: If there are any outstanding patches available on the machine, this indicator will show as *Not Compliant*. Otherwise, if the device is updated with the latest available updates, this indicator will show as *Compliant*.
- **Firewall**: If any of the Private, Public, or Domain Firewall policies are applied to the device, it will show as *Compliant*. If any of the above-mentioned policies are not applied to the device, it will show as *Non-Compliant.*
- **EPP**: If the antivirus is not installed or if the antivirus services are running, this will show as *Not Compliant*. Otherwise, if the antivirus is installed and running, it will show as *Compliant*.
- **Windows Remote Desktop:** If Remote Desktop connection is enabled on the device, this will show as *Not Compliant.* Otherwise, if the Remote Desktop connection is not allowed, this will show as *Compliant*.

- **3rd party Apps:** If an update is available for any of the BigFix supported 3rd-party apps installed on the device, it show as *Not Compliant. Otherwise,* if the 3rd-party apps installed on the device are updated with the latest patch level, this indicator will show *Compliant*.
- **File Backup:** If One Drive Backup is NOT enabled, this will show as *Not Compliant.* Otherwise, if One Drive Backup is enabled on the device, it will show as *Compliant*.
- **Disk Encryption**: If the C-drive of the device is not encrypted with Bitlocker, this indicator will show as *Not Compliant.* Otherwise, if the C-drive is encrypted with BitLocker, it will show as *Compliant.*

Steps to configure Device Status Widget are as follows:

1. Go to External Site – BigFix Resolve – Use Configure Device Status Task.
2. To configure the page for compliance checks on each of the following, select the relevant options from each dropdown:

- EPP (End-point Protection) has 3 fields to check and configure for compliance for Anti-virus:
  - Symantec
  - Windows Defender
  - McAfee

  Select each option to check which one is applicable in your environment, which will check if Antivirus is installed and running.
- Operation System Compliance has 3 options that allow the end user to check the OS for patch compliance:
  - Outstanding OS patches
  - Outstanding OS and Windows Application patches
  - Custom Sitename

    A custom site in BigFix refers to a site that contains custom content and actions specific to an organization's needs.

    Custom sites can be created to manage endpoints in a particular department or location, to deploy specific software or patches, or to enforce particular security

policies. They can contain custom fixlets, tasks, analyses, and dashboards that provide a tailored view of endpoint activity and compliance.

By creating custom sites, organizations can effectively manage and secure their endpoints in a way that meets their specific needs and requirements.

(Provide the name and URL of the custom sitenames in the relevant dialogue boxes).

Based on the results, select the OS compliance status in the console for the machine being used.

- Compliance for third-party applications has 2 options which allow us to check and enforce compliance. To check, select the relevant option from the console:

Note that this is only applicable for Windows applications which are supported on BigFix as well

- Relevant patches from Windows applications (Which includes – Windows Application and Extended Patches).
- Check from Custom Site name (provide the name and URL of the custom site names in the relevant dialogue boxes and the site should be available on the console)

2.2.1.4 Configure Support Icon

1. Go to External Site – BigFix Resolve – Use Configure Support Widget Task.
2. To configure the relevant buttons on the dashboard, provide the Email address, Chat hyperlink, and helpdesk number of the support team. And run the action against all the endpoints where Assistant Tab is Installed.

2.2.2 Ticket

The BigFix Resolve WebApp is used for integration with ServiceNow, so if anyone wants to configure it, they can do so by using Fixlet - Install BigFix Resolve Client Dashboard (Assistant & Tickets Fixlet). If the organization doesn't want to use the resolve WebApp, they can only use Fixlet - Install BigFix Resolve Client Dashboard Assistant Fixlet.

1. Go to External Site – BigFix Resolve – Use Configure Ticket Tab task.
2. To Configure ticket tab – Please Input the FQDN* and Port Number of the Server Where BigFix WebApp is Installed.

Fully Qualified Domain Name

2.3 Catalog of Healing BigFix Fixlets

BigFix Resolves provides a list of out of the box fixlets that can be differently categorized into two main categories:

- **Self-service remediation**: These are one click solution fixlets that user can execute to resolve different type of issues related to device performance improvement, remediation of application issues, remediation of compliance problems or optimization of the device.
- **Self-healing tasks:** These are fixlets deployed by the IT Operator to enforce certain configurations, settings or to guarantee that some processes are always up and running into the end user device**.**

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property

Department in your country or send inquiries, in writing, to:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

HCL Technologies ltd. Provides this publication "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of non-infringement, merchantability or fitness for a particular purpose. Some jurisdictions do not allow disclaimer of

express or implied warranties in certain transactions, therefore, this statement may not apply to you. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk. HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

cclxxxiii

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under

terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us. The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-

HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind.

HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).

Portions of this code are derived from HCL Ltd. Sample Programs.

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

cclxxxv

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED.

"AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.