opentext™

OpenText™ Server Backup Portal 9.5

Installation and Configuration Guide

Document History

Version	Date	Description
1	January 2026	Initial installation and configuration guide for Portal 9.5*x*. Includes updates to Manage the Portal AMP Proxy certificate.

Table of Contents

1 Introduction to Portal 8

1.1 System Overview 8

1.1.1 Front-end components (web accessible) 8

1.1.2 Back-end components (not externally accessible) 9

1.2 Portal – Distributed System (recommended) 10

1.3 Portal – Single System 11

2 Prerequisites and recommendations 13

2.1 Software prerequisites 13

2.1.1 Software prerequisites for a distributed system 13

2.1.2 Software prerequisites for a single system 14

2.2 Default ports 15

2.3 SQL Server requirements 16

2.4 UNC location for saving agent installers 17

2.5 URLs for validating agent installers 17

2.6 Security recommendations 18

2.6.1 Disable cipher suites with RSA encryption 18

2.6.2 Configure IIS to enforce HSTS for the Portal website 18

2.6.3 Prohibit unprivileged access to Portal front-end servers 19

2.6.4 Disable the default website 19

2.6.5 Enable the request smuggling filter 20

3 Install Portal 21

3.1 Install Portal as a distributed system 21

3.1.1 Install back-end system components 21

3.1.2 Install front-end system components 24

3.1.3 Install AMP Proxies and Redirectors 28

3.1.4 (Recommended) Configure Windows authentication for database access 30
3.2 Install Portal on a single system 33
4 Manage the Portal AMP Proxy certificate 37
4.1 Check the Portal AMP Proxy certificate type and expiry date 37
4.2 Replace the Portal AMP Proxy certificate 39
4.2.1 Roll back to a previous Portal AMP Proxy certificate 41
4.3 Generate a Certificate Signing Request with the same public key as the current certificate 42
4.4 Extend the validity period of the self-signed Portal AMP Proxy certificate 43
5 Integrate Portal with EVault Reports 45
5.1 Enable Reports integration in Portal 45
5.2 Associate customer short names with Portal sites 46
6 Set up, enable or disable Portal features 47
6.1 Set up the data deletion feature 47
6.1.1 Configure Portal to use TLS 1.2 for vault data deletion requests 47
6.2 Enable or disable Portal features 47
6.3 Enable the skipped rate feature 49
6.4 Enable or disable the Create New Site wizard 51
6.5 Set up two-factor account verification 52
6.5.1 Require users to set up two-factor account verification 52
6.6 Display a new features list on the Sign In page 54
6.6.1 Revise the new features list 54
6.6.2 Display the new features list on the Sign In page 56
6.6.3 Hide the new features list on the Sign In page 57
7 Set up emailed reports and automatic emails 58
7.1 Customize automatic emails 58
7.1.1 Customize welcome emails for setting Portal passwords 59
7.1.2 Customize password reset emails 61

7.1.3 Change the Support phone number in password-related emails 63
7.1.4 Customize backup notification emails 64
7.1.5 Customize emails for encryption password changes 66
7.1.6 Customize data deletion emails 68
7.1.7 Customize agent auto upgrade emails 72

8 Configure Portal 75

8.1 Configure Portal SSL use 75
8.1.1 Configure Portal to not use SSL 75
8.1.2 Configure Portal to use SSL 76
8.2 Specify privacy policy URLs 77
8.3 Configure a web farm 78
8.4 Configure load balancing for multiple Redirectors 80
8.4.1 Health check endpoint for AMP Redirector 80
8.4.2 Configure the Redirector Health Check Endpoint 81
8.4.3 Example: Configure a load balancer for AMP Redirectors 82
8.5 Configure load balancing for multiple Notification services 88
8.5.1 Example: Configure a load balancer for Notification services 88

9 Modify Portal 97

9.1 Convert Portal from a single system to a two-server distributed system 98
9.2 Install additional Redirectors 101
9.3 Install additional Notification services 102

10 Upgrade Portal 104

10.1 Prepare for a Portal upgrade 104
10.2 Upgrade Portal components 105
10.3 Verify the upgraded Portal and make it available to users 106
10.4 Roll back databases after a failed upgrade 106

11 Validate the Portal installation 107

11.1 Log in to Portal for the first time 107

11.2 Create a site 107
11.3 Create an Admin user 108
11.4 Add a computer 108
11.5 Add a backup job 109
11.6 View the Reports tab 110

12 Troubleshooting and Maintenance 111

12.1 Redirecting Ports 111
12.2 SQL database installation failure 113
12.3 Agent doesn't register to Redirector 113
12.4 "Unauthorized proxy" errors 114
12.5 Agents go offline sporadically 114
12.6 Cannot load type when loading Portal login page 115
12.7 NT AUTHORITY\SYSTEM login fails when navigating to Portal 115
12.8 403 error when attempting to open the Portal website 115
12.9 IIS default page appears instead of Portal sign-in page 115
12.10 Database transaction log files require monitoring 116

13 Portal Disaster Recovery 117

13.1 Back up a distributed Portal instance 117
13.2 Restore SQL Server for a distributed Portal instance 117
13.3 Restore a distributed Portal instance 118
13.4 Back up Portal on a single system 118
13.5 Restore Portal on a single system 119

14 OpenText Server Backup Support 120

14.1 Contacting OpenText 120

Appendix A Configure single sign-on 121

A1 Configure single sign-on in Portal 122
A1a. Configure Portal to use a federated identity server 122
A1b. Install IdP Signing Certificate on the machine where Portal is installed 124

A1c. Username in the SAML token 124
A1d. User role in the SAML token 125
A1e. User site in the SAML token 126
A1f. SAML token/Expected claims 126
A2 Configure single sign-on using Microsoft Entra ID 129
A2a. Prerequisites 129
A2b. Set up groups and users in Entra ID 130
A2c. Create an enterprise application in Entra ID 131
A2d. Set up certificate and configuration values 137
A3 Troubleshoot single sign-on 138

1 Introduction to Portal

OpenText Server Backup Portal is a web-based interface that provides a centralized point of control for managing backups and restores of servers on large computer networks.

Portal is scalable and can accommodate a variety of different-sized organizations. A simple system can run on a single computer and efficiently handle approximately 500 computers. A distributed system can handle much larger organizations with tens of thousands of computers.

This guide describes how to install and configure Portal. Information on creating backups and restores is not part of this guide but can be found in the Portal online help.

1.1 System Overview

Portal includes the front-end and back-end components described in the following tables. These components can be installed as a distributed system (recommended) or on a single server.

1.1.1 Front-end components (web accessible)

Component	Description
Portal UI	Browser-based interface that allows users to manage backups and restores of servers on large computer networks. Portal UI also allows for reports generation as well as access to status feeds and collaborative capability between users in the same company.
AMP Redirector Service	Accepts agent registrations and balances the number of authorized agents between available proxies in the Portal environment. Beginning in Portal 9.10, you can install multiple Redirectors behind a load balancer in a distributed Portal environment.
Load Balancer	A load balancer (not provided with Portal) can be installed to balance the load across multiple Portal front-end systems. A load balancer is also required if you want to install multiple Redirectors or Notification services in a distributed Portal environment. You can configure a load balancer to check the health of each Redirector service and only route requests to healthy services, and to route requests to available Notification services.

Component	Description
AMP Proxy	Acts as the access point for agents to connect to the Portal environment. It passes messages between the agent and the backend services as well as messages from the UI to the agent allowing for configuration of the Agent as well as status uploads from the agent. Multiple AMP Proxy servers can be used to increase the number of Agents the overall environment can support. 1800 agents are supported per AMP Proxy.
Portal Service Connector	Provides internal communication between the Portal UI and the backend services/database.
Host Protect Service	Provides internal communication between the Portal UI and the backend services/database.
API Scheduler	Runs periodically to clean up database tables, send out email notifications and process data deletions.
Task Scheduler	Executes scheduled reports as well as other back-end tasks that are executed on a schedule.

1.1.2 Back-end components (not externally accessible)

Component	Description
SQL Databases	• WebCC database— Contains Agent content information. • UserManagement database— Contains User Management information. • SiteManagement database— Contains site-specific content information. • EVaultWeb database— Contains user content information. *Note:* Beginning in version 9.30, a database named “HangFire” is also installed with Portal. This database was added in preparation for a feature that is not yet available.
Task Service	Flags scheduled backups that are missed. This component is installed with the SQL databases.
Notification Service	Allows Agents to notify the UI of Agent configurations, jobs statuses, and other information.
Registration Service	Allows Agents to register with Portal.

Component	Description
Status	Reports on the running state of some back-end services (e.g., Notification and Registration).

Note: The Propagation Service is no longer available or necessary.

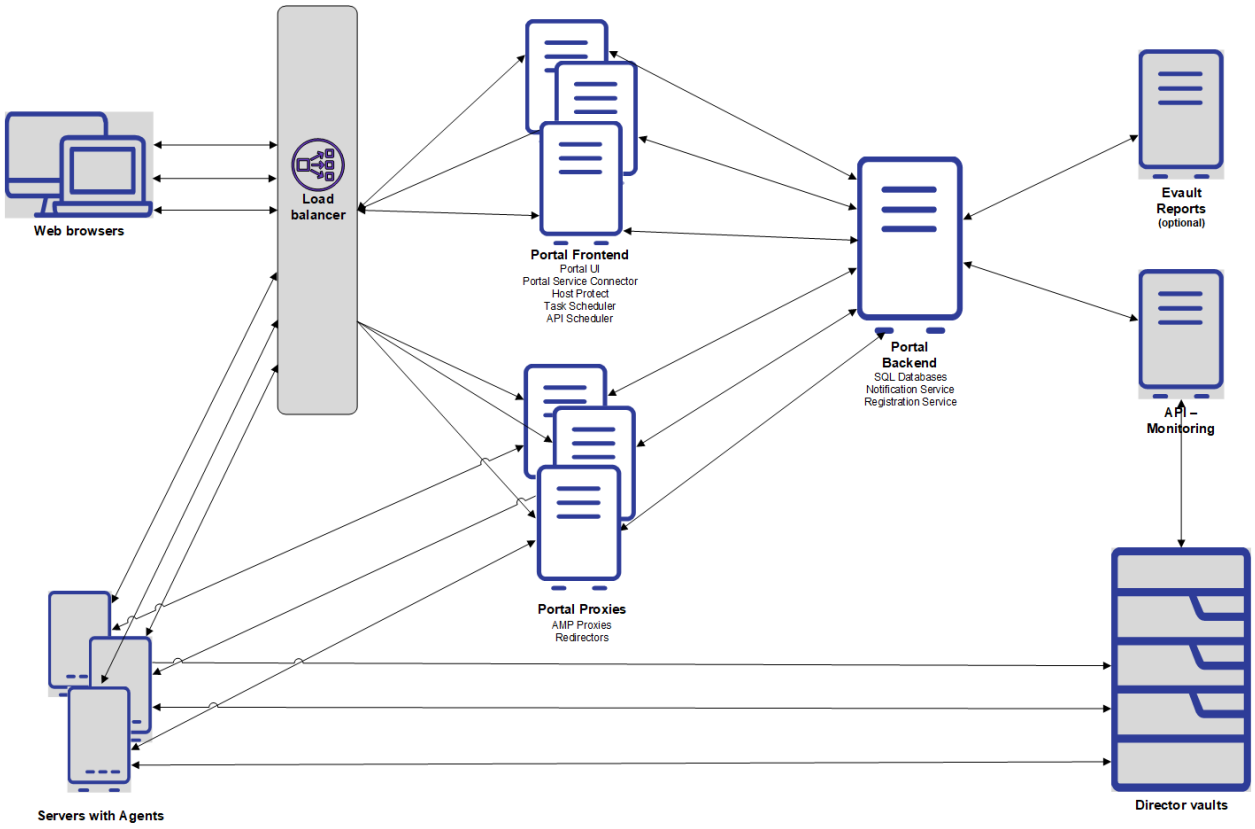
1.2 Portal – Distributed System (recommended)

You can install Portal as a distributed system that can be scaled out to handle a large number of agents and users. Figure 1 shows an example of a distributed Portal system, with multiple Portal front-end servers, Proxies and Redirectors.

Notes:

- The Load Balancer is optional and is not provided by OpenText.
- By default, only three reports are available in Portal. For additional reports, EVault Reports must be integrated with Portal. See Integrate Portal with EVault Reports.
- To delete data from Director vaults in response to requests from Portal and to remotely monitor protected data using API calls, API – Monitoring must be integrated with Portal. See Set up the data deletion feature and the *API – Monitoring Installation and Usage Guide*.

Figure 1 Portal – Distributed System



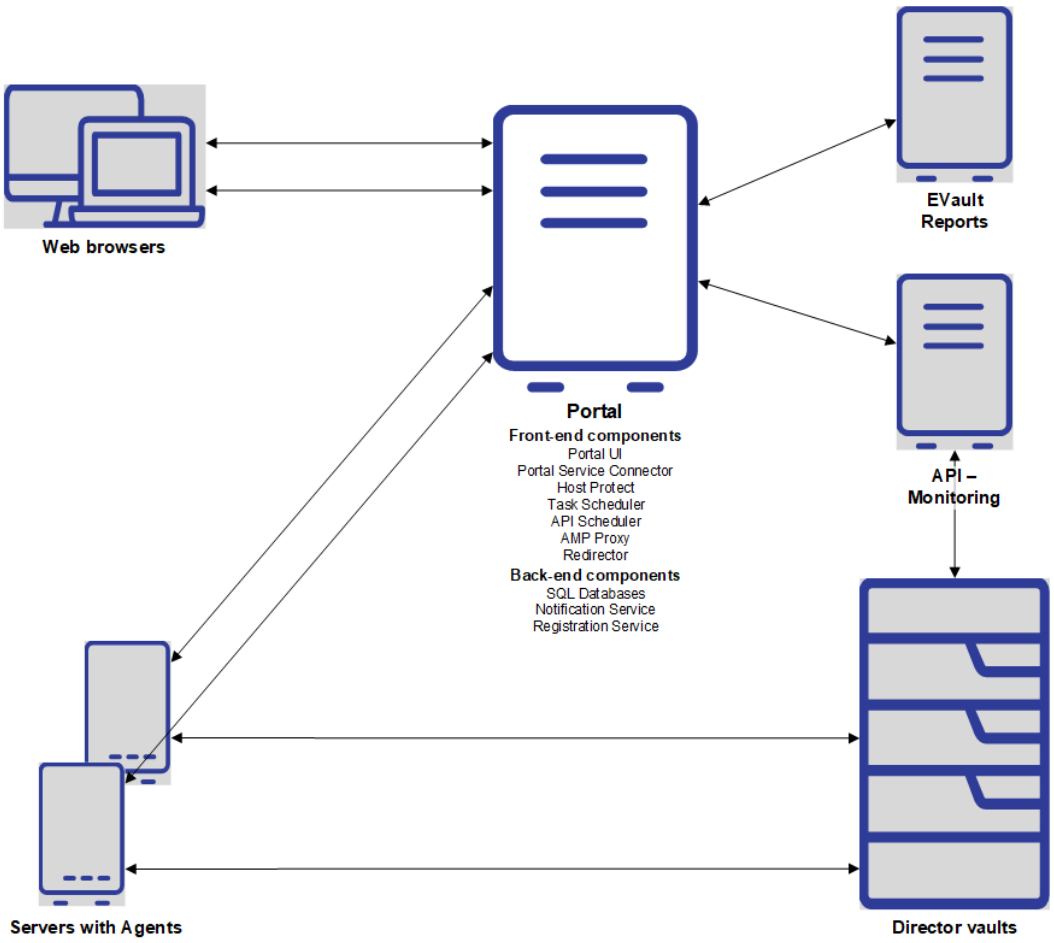
1.3 Portal – Single System

The single Portal system shown in Figure 2 is not recommended, but can be used for environments with fewer than 500 agents.

Notes:

- By default, only three reports are available in Portal. For additional reports, EVault Reports must be integrated with Portal. See Integrate Portal with EVault Reports.
- To delete data from Director vaults in response to requests from Portal and to remotely monitor protected data using API calls, API – Monitoring must be integrated with Portal. See Set up the data deletion feature and the *API – Monitoring Installation and Usage Guide*.

Figure 2 Portal – Single System



2 Prerequisites and recommendations

As described in System Overview, Portal components can be installed as a distributed system (recommended) or on a single server.

All components must be installed on a supported 64-bit operating system. For a list of supported platforms, see the Portal release notes.

On each system where Portal components will be installed, do the following:

- Turn off IPV6.
- Use IPV4 addresses when providing settings for IP addresses.
- Make sure all servers are set to the same time zone and have the same time.
- Install required software prerequisites. See Software prerequisites.
- If Portal components are installed as a distributed system, open the required ports. For more information, see Default ports.

For increased security we recommend disabling older cipher suites on systems where Portal components are installed. See Security recommendations.

2.1 Software prerequisites

2.1.1 Software prerequisites for a distributed system

If you are installing Portal components as a distributed system (recommended), the following table shows prerequisites that are required on each system.

System	Prerequisite

Portal UI (front-end)	Web Server (IIS) 8.0 or later, including all role services that are installed by default, plus the following available role services and features:
	• Under Common HTTP Features:
	  ○ Static Content
	  ○ HTTP Errors
	  ○ HTTP Redirection
	• Under Application Development:
	  ○ .NET Extensibility 4.8 or later
	  ○ ASP.NET 4.*x*
	  ○ ISAPI Extensions
	  ○ ISAPI Filters
	• Under Security:
	  ○ Windows Authentication

System	Prerequisite
	Under .NET Framework 4.*x* Features: • .NET Framework 4.*x* • ASP.NET 4.*x* • HTTP Activation
	.NET Framework 4.8
AMP Proxy and Redirector	.NET Framework 4.8
Databases	Microsoft SQL Server or SQL Server Express 2022, 2019, 2017, 2016 or 2014 (64-bit) installed with mixed mode authentication and case-insensitive collation and running. The latest SQL Server service packs and updates are recommended. For detailed information, see SQL Server Requirements.
	.NET Framework 4.8

Web services, including Notification, Registration and Status (back-end)	Web Server (IIS) 8.0 or later, including all role services that are installed by default, plus the following available role services:
	• Under Common HTTP Features:
	  ○ Static Content
	  ○ HTTP Errors
	  ○ HTTP Redirection
	• Under Application Development:
	  ○ .NET Extensibility 4.8 or later
	  ○ ASP.NET 4.*x*
	  ○ ISAPI Extensions
	  ○ ISAPI Filters
	• Under Security:
	  ○ Windows Authentication

	Under .NET Framework 4.*x* Features: • .NET Framework 4.*x* • ASP.NET 4.*x* • HTTP Activation
	.NET Framework 4.8

2.1.2 Software prerequisites for a single system

The following software must be installed before you can install Portal on a single system:

- Web Server (IIS) 8.0 or later, including all role services that are installed by default, plus the following available role services and features:
  - Under Common HTTP Features:

        - Static Content
        - HTTP Errors
        - HTTP Redirection
    - Under Application Development:
        - .NET Extensibility 4.8 or later
        - ASP.NET 4.*x*
        - ISAPI Extensions
        - ISAPI Filters

      Note: Make certain that ASP.NET and .NET Extensibility are turned on in Windows features, particularly if IIS is installed before ASP.NET.
    - Under Security:
        - Windows Authentication

- Under .NET Framework 4.*x* Features:
    - .NET Framework 4.*x*
    - ASP.NET 4.*x*
    - HTTP Activation
- .NET Framework 4.8
- Microsoft SQL Server or SQL Server Express 2022, 2019, 2017, 2016 or 2014 (64-bit) installed with mixed mode authentication and case-insensitive collation and running. For detailed information, see SQL Server requirements.

2.2 Default ports

The following table shows default ports that must be open to enable communication between Portal components installed as a distributed system (recommended).

System	Port	Communication
Portal UI (front-end)	Outbound: 6502	To AMP Proxy
	Outbound: 1433	To Database
	Outbound: 80	To Server Backup Reports token manager (if used)
	Outbound: 1433	To Server Backup Reports database (if used)
AMP proxy	Outbound: 80	To Web services (back-end)
	Outbound: 1433	To Database
	Inbound: 6502	From Portal UI
	Inbound: 8087	From agents
Redirector	Outbound: 80	To Web services
	Outbound: 1433	To Database
	Inbound: 8086	From agents

System	Port	Communication
Databases	Inbound: 1433	From Portal UI
		From AMP Proxy
		From Redirector
Web services, including Notification and Registration (back-end)	Outbound: 6502	To AMP Proxy
	Inbound: 80	From AMP Proxy
		From Redirector
Agents (computers)	Outbound: 8087	To AMP Proxy
	Outbound: 8086	To Redirector
	Outbound: 443	To Portal (for automatic agent upgrades)

2.3 SQL Server requirements

For new Portal installations, a supported Microsoft SQL Server version must be installed and running, with the following requirements:

SQL Server Option	Requirement
Instance feature	Database Engine Services
Authentication	Mixed Mode (SQL Server and Windows authentication)
Collation	Any case-insensitive collation
Instance name	Any instance name; no restrictions

SQL Server should be installed on a system that is not externally visible, configured with default settings, and ready for use.

To ensure secure communications between SQL Server and Portal, we recommend enabling TLS in the SQL Server instance. To do this, add a certificate to SQL Server and configure the server to force encryptions as described in Microsoft documentation: Configure SQL Server Database Engine for encrypting connections. Optionally, you can also add `Encrypt=True;TrustServerCertificate=True` in all database connection strings in Portal configuration files, as shown in the following example:

```
<add name="WebCC.Sql.Connection" connectionString="Data
Source='PORTALSQL';Database='WebCC';User
ID='user';Password='password';
Encrypt=True;TrustServerCertificate=True"
providerName="System.Data.SqlClient" />
```

For a list of Portal configuration files with database connection strings, see Configuration files with database connection strings.

When SQL Server and Portal services are installed on different servers, TCP/IP must be enabled for the database instance. SQL credentials must also be specified for connecting to the database from remote servers.

To install Portal with a remote SQL Server, install the sqlcmd utility from Microsoft on the machine where you are installing Portal. See sqlcmd Utility documentation from Microsoft. Otherwise, a "failure to create database" error might occur during the installation.

During installation, you must specify a user for connecting to SQL Server. This user must have permission to access the master, model, Msdb and tempdb databases (DBOwner). When Windows authentication is used for connecting to SQL Server during installation, the sysadmin server role must be enabled for the NT AUTHORITY/SYSTEM login.

The password for the SQL Server user should not include semicolons, single quotation marks or double quotation marks.

Be sure that the Autogrowth setting for each Portal database data and log file is sufficient. If the Autogrowth setting is too low, Portal performance could be affected. For more information, see documentation from Microsoft: Considerations for the autogrow and autoshrink - SQL Server

Portal can use the same SQL Server instance as Server Backup Reports. However, for scalability and environments with many agents and vaults, it is preferable to use separate SQL Server instances for Portal and Reports.

2.4 UNC location for saving agent installers

Installers for automatically upgrading agents on Windows computers can be provided through Portal. A UNC location is required for saving the agent installers.

2.5 URLs for validating agent installers

To validate installers for automatically upgrading Windows agents, Portal UI servers must have Internet access. At minimum, each Portal UI server must have access to the URLs for validating Windows Agent installation kit certificates and intermediate certificates.

For Windows Agent 9.30 and later installation kits, the following URLs are required for certificate validation:

- http://crl.sectigo.com/
- http://crl.comodoca.com/

For Windows Agent 9.20 and earlier installation kits, the following URLs are required for certificate validation:

- http://sw.symcb.com
- http://crl3.digicert.com

- http://crl4.digicert.com

For Windows Agent installation kits that are re-signed with another service provider's certificate, you must determine the CRL URLs (CRL Distribution Points).

If an agent is installed on a server that does not have access to these URLs, the agent cannot be upgraded automatically.

For automatic Windows Agent upgrades if Portal is using a self-signed certificate, the same self-signed certificate should be exported from the Portal server and imported on each Agent server.

2.6 Security recommendations

2.6.1 Disable cipher suites with RSA encryption

On Portal systems which are exposed to the internet, we recommend disabling cipher suites which include RSA encryption.

Typically, systems where the Portal UI, Proxy or Redirector are installed are exposed to the internet. However, if a load balancer handles https connections to the Portal UI, you do not need to disable cipher suites on the Portal UI system.

We recommend disabling cipher suites with names that start with TLS_RSA_*. You do not need to disable cipher suites that use RSA signatures and include DHE or ECDHE in their names (i.e., names that begin with "TLS_ECDHE_RSA_" or "TLS_DHE_RSA_").

Note: Disabling these cipher suites could cause older Agents to lose connection with Portal, but newer Agent versions will remain connected. Disabling cipher suites could also cause problems with other software on the web servers.

For instructions on disabling cipher suites, see Microsoft documentation: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/manage-ssl-protocols-in-ad-fs#enabling-or-disabling-additional-cipher-suites

2.6.2 Configure IIS to enforce HSTS for the Portal website

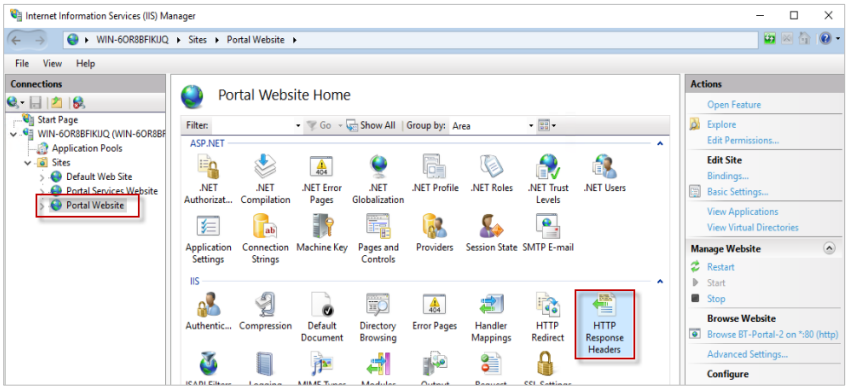
On each Portal UI server, configure IIS to enforce HSTS (HTTP Strict Transport Security) on the Portal website. HSTS specifies that connections must be made using HTTPS instead of HTTP.

IMPORTANT: Do the following on each server where the Portal UI is installed.

To configure IIS to enforce HSTS for the Portal website:

1. On the Portal UI server, open the Internet Information Services (IIS) Manager.

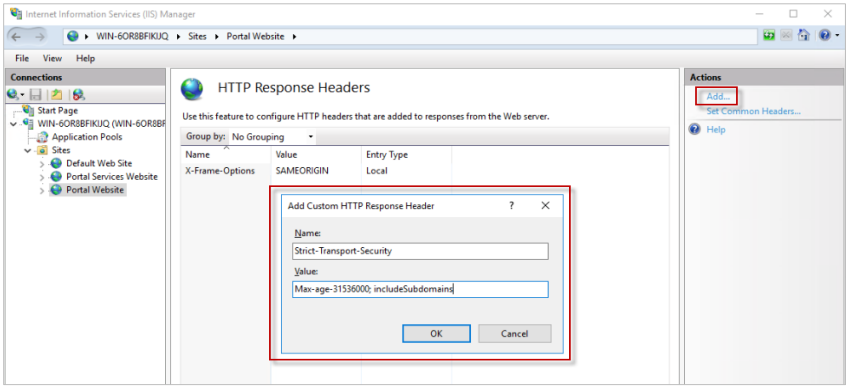
2. In the left pane of the IIS Manager, expand the Sites list and click **Portal Website**.
3. In the center pane of the IIS Manager, double-click **HTTP Response Headers**.



4. In the HTTPS Response Headers Actions pane, click **Add.**
5. In the Add Custom HTTP Response Header box, specify the values shown in this table:

Field	Value
Name	Strict-Transport-Security
Value	Max-age=31536000; includeSubdomains

6. Click **OK**.



2.6.3 Prohibit unprivileged access to Portal front-end servers

Do not allow any unprivileged access to Portal front-end servers. Allowing unprivileged access to a Portal front-end server could expose the system to security vulnerabilities.

For security reasons, the Portal Services Website must only be bound to 127.0.0.1 (localhost) and must not be exposed on the internet.

2.6.4 Disable the default website

On a Portal UI server, disable the default website if it is unused and disable any other unused websites in the IIS configuration. An unused website could serve a default IIS page, which can be security issue.

2.6.5 Enable the request smuggling filter

We recommend enabling the request smuggling filter on Portal UI servers. For more information, see HTTP Request Smuggling in Microsoft IIS Server.

3 Install Portal

We recommend installing Portal as a distributed system, with components on multiple systems. See Install Portal on a distributed system.

You can also install all Portal components on one machine. A single Portal system is not recommended, but can be used for environments with fewer than 500 Agents. See Install Portal on a single system.

After installing Portal, we recommend that you validate the installation. See Validate the Portal installation. If problems occur, see Troubleshooting and Maintenance for possible solutions.

After Portal is installed, you can set up additional features as described in Integrate Portal with EVault Reports, Set up the data deletion feature and Set up emailed reports and automatic emails. For additional configuration options, see Configure Portal.

3.1 Install Portal as a distributed system

To install Portal as a distributed system, do the following:

- Install back-end system components

  Note: Beginning in Portal 8.88, when you install back-end Portal components on a server, the installer creates a PortalKey.txt file that contains a machine key for Portal configuration files. This file is required when you install Portal front-end components on another server. Be sure to keep a backup copy of this file somewhere safe.

- Install front-end system components
- Install AMP Proxies and Redirectors
- (Recommended) Configure Windows authentication for database access

3.1.1 Install back-end system components

When installing Portal as a distributed system, you must first install the back-end system components:

- Databases
- Notification service
- Registration service

You can also install the optional Status component.

The website where the Notification and Registration services are installed must only be accessible from within the local network (specifically, from the systems where the Proxy and the Redirector are installed). It must not be available over the internet. Agents do not need to connect to these services directly.

Beginning in Portal 9.20, you can install multiple Notification services in a distributed Portal environment. To install an additional Notification service and configure a load balancer to route requests to available Notification services, see Install additional Notification services and Configure load balancing for multiple Notification services.

To install back-end system components:

1. On the system where you want to install back-end Portal components, log in as an administrator and run the Portal installation kit.
2. On the Welcome page, click **Next**.
3. On the View Notes page, click **Next**.
4. On the License Agreement page, read the license agreement. Select **I accept the terms of the license agreement**, and then click **Next**.
5. On the SQL Server Setup page, choose the SQL Server instance where the databases will be installed. Specify the authentication method, and then click **Next**.

   The databases can be installed using Windows authentication. To use Windows authentication, you must be logged in as a user with full access to the database server.

   (Optional) Click **Test Connection** to validate your connection with the database server.

   Notes:

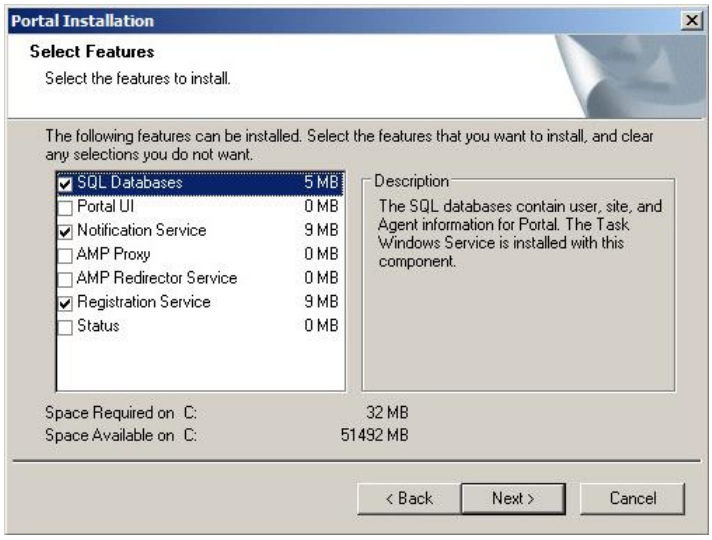
   - The SQL Server instance must have been installed with mixed mode authentication.
   - The SQL Server instance cannot contain existing EVaultWeb, WebCC, UserManagement, or SiteManagement databases.
   - If you want to install Portal with a remote SQL Server, install the sqlcmd utility from Microsoft on the machine where you are installing Portal. Otherwise, a "failure to create database" error might occur during the installation.
6. On the Select Features page, select the following components, and then click **Next**:

   - SQL Databases

     Note: The Task Service is installed with the SQL databases.

   - Notification Service
   - Registration Service

   You can also select the optional Status component.



7. If you are installing the optional Status component, the Domain Name page appears. On this page, specify the Portal domain name, protocol (http/https) and port, and then click **Next**. This is the address which your end users will use to connect to Portal.

   Note: The Domain Name page does not appear unless you are installing the Status component.

8. On the Notification and Registration Configuration page, enter the IP address that the Proxy and Redirector will use to access the Notification and Registration services, and then click **Next**.

9. On the Notification Service – Locations and Virtual Directory page, specify the following Notification service information, and then click **Next**:

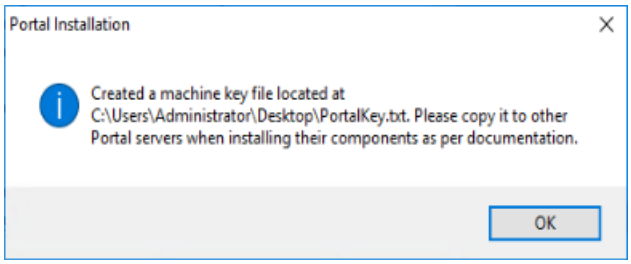
   - Installation location
   - Log file location. For security reasons, the log files should not be under the same path where the Notification service is installed.
   - Virtual Directory Name. Change this name if it will conflict with another already installed website/service. If you change the virtual directory name, record it. You will need to enter it when installing the proxy.

10. On the Registration Service – Locations and Virtual Directory page, specify the following information, and then click **Next**:

    - Installation location
    - Log file location
    - Virtual Directory Name. Change this name if it will conflict with another already installed website/service. If you change the virtual directory name, record it. You will need to enter it when installing the proxy.

11. On the Services/Support Files page, specify the location for installing services and support files, and then click **Next**.
12. In the confirmation dialog box, click **Yes**.
13. When a dialog box states that a machine key file has been created, note the location of the PortalKey.txt file, and then click **OK**.

    IMPORTANT: You will need the PortalKey.txt file when installing Portal front-end components on other servers. Be sure to keep a backup copy of this file somewhere safe.

    After Portal components are installed, a Component Status page appears. This page indicates which components have been installed and which components need to be installed before the system will be operational.

    The page also indicates if one of the components is not at the same versions as the other components and will need to be upgraded. Components which are currently installed, but are not up to the current version, may show as missing.

    To save a copy of the Component Status information, enter a location for saving the file, and then click **Save**.
14. Click **Next**.
15. On the Portal Installation Successful page, click **Finish**.

3.1.2 Install front-end system components

After installing back-end system components on one server, you can install front-end system components on another server.

Front-end system components include the Portal UI and the following components that are installed with the Portal UI: Portal Service Connector, Host Protect Service, and Task Scheduler.

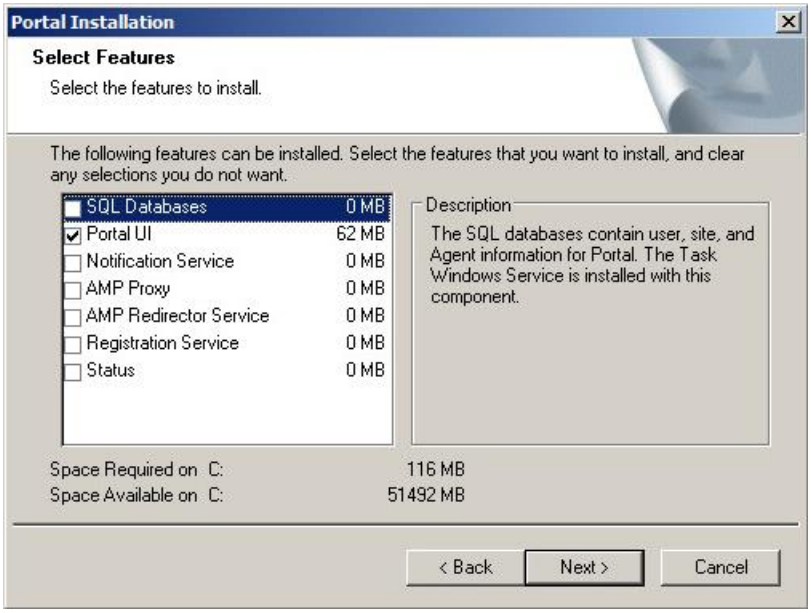
IMPORTANT: The PortalKey.txt file created when you installed back-end Portal components is required for installing Portal front-end components on another server. This file contains a machine key for Portal configuration files. Be sure to keep a backup copy of this file somewhere safe.

Note: If you want to install front-end system components on more than one server, see Configure a web farm for additional installation and configuration information.

To install front-end system components:

1. On the system where you want to install front-end Portal components, log in as an administrator.
2. Copy the Portal installation kit to the server.
3. Copy the PortalKey.txt file created in Install back-end system components to the server.
4. Run the Portal installation kit.
5. On the Welcome page, click **Next**.
6. On the View Notes page, click **Next**.
7. On the License Agreement page, read the license agreement. Select **I accept the terms of the license agreement**, and then click **Next**.
8. On the SQL Server Setup page, specify the SQL Server instance where the databases are installed. Specify the authentication method, and then click **Next**.

   You can optionally click **Test** to validate your connection with the database server.
9. On the Select Features page, select **Portal UI**, and then click **Next**.



10. On the Language Selection page, select languages for displaying Portal text, and then click **Next**. In addition to the default English (United States), you can select English (United Kingdom), French, German and Spanish

    Note: When Portal is viewed in English (United Kingdom), times are shown in 24-hour clock format.

    If you do not install a language now, you can add it later by rerunning the installation in Modify mode. You can also remove a language this way.

11. On the Domain Name page, specify the Portal domain name and port, and then click **Next**.

    On this page, you can provide the domain name for Portal, as well as the protocol to use (http/https). This specifies the address for users to connect to Portal.

    If a load balancer will handle https connections to the Portal UI, install Portal with the http protocol and change the configuration to not use SSL. See Configure Portal to not use SSL. If you use a load balancer and install Portal with the https protocol, attempts to reach the site will fail with a redirection error.

    If a load balancer is not used, we highly recommend that you install Portal with the https protocol. For https, a signed certificate must be applied to the website where this application is installed. Make sure that the certificate matches the domain name that you are using for Portal, and import the certificate into IIS after the Portal installation is complete.

    Note: Beginning in version 8.85, Portal uses SSL by default. While it is not recommended (unless a load balancer will handle https connections to the Portal UI), you can configure Portal to not use SSL. See Configure Portal to not use SSL.

    When configuring the system for external access, the domain name that is provided here should be the name which is registered on the internet for Portal. If the system is being set up before external access is configured, the application will only work after you successfully set up the domain name that has been provided here. If the domain name changes after installation, the installed components will need to be manually updated.

12. On the Portal – Select Installation and Log Paths page, specify the Portal installation location and Logs location, and then click **Next**.

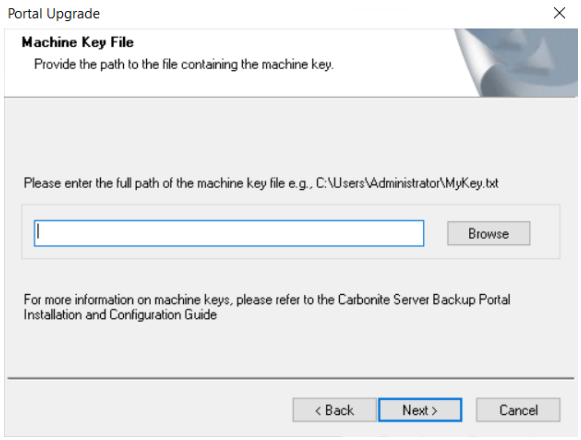
13. On the Portal Service Connector – Location and Virtual Directory page, specify the following information, and then click **Next**:

    - Installation location
    - Log file location
    - Virtual Directory Name. Change this name if it will conflict with another already installed website/service.

14. On the Host Protect – Location and Virtual Directory page, specify the following information, and then click **Next**:

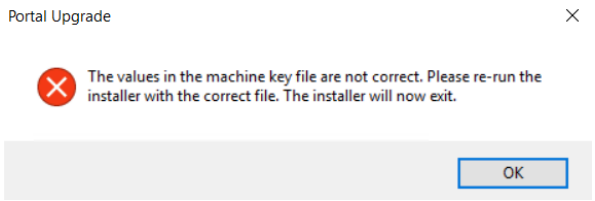
    - Installation location
    - Log file location
    - Virtual Directory Name. Change this name if it will conflict with another already installed website/service.

15. On the API Scheduler Installation page, specify the following information, and then click **Next**:
    - Installation location
    - Log file location
16. On the Task Scheduler – Select Installation Path page, specify the Task Scheduler installation location and log file location, and then click **Next**.
17. On the Machine Key File page, specify the full path and file name of the PortalKey.txt file that you copied to the server in Step 3, and then click **Next**.



The installer checks the PortalKey.txt file. If the file contains a valid machine key, the installation continues.

If there is a problem with the PortalKey.txt file, the following message appears. Please check the file and try the installation again.



18. In the confirmation dialog box, click **Yes**.

    The installation begins.

    After the components are installed, a Component Status page appears. This page indicates which components have been installed, and which components need to be installed before the system will be operational.

    The page also indicates if one of the components is not at the same versions as the other components and will still need to be upgraded. Components which are currently installed, but are not up to the current version, may show as missing.

To save a copy of the Component Status information, enter a location for saving the file, and then click **Save**.

19. Click **Next**.
20. On the Portal Installation Successful page, click **Finish**.

    A message states that sensitive information is now encrypted using the machine key. Be sure to keep a backup copy of the PortalKey.txt file somewhere safe.

3.1.3 Install AMP Proxies and Redirectors

When installing Portal as a distributed system, the final components to install are the AMP Proxies and Redirectors.

Multiple proxy systems can be set up for the same Portal environment. Each proxy supports up to 1800 agent connections.

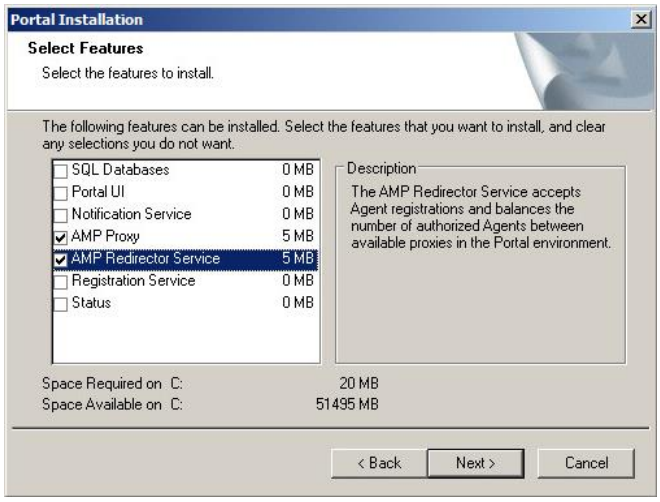
Beginning in Portal 9.10, you can install multiple Redirectors in a distributed Portal environment. To configure a load balancer to check the health of each Redirector service and only route requests to healthy services, see Configure load balancing for multiple Redirectors.

The Redirectors and Proxies need to be accessible by all agents connecting to your environment. For environments which will support both local network (LAN) internet connected agents, all agents need to have access to the same domain names/IP addresses for the Proxy.

To install the Proxy and Redirector:

1. On the server where you want to install the Proxy and Redirector, log in as an administrator.
2. Copy the Portal installation kit to the server.
3. Copy the PortalKey.txt file created in Install back-end system components to the server.
4. Run the Portal installation kit.
5. On the Welcome page, click **Next**.
6. On the View Notes page, click **Next**.
7. On the Software License Agreement page, read the license agreement. Select **I accept the terms of the license agreement**, and then click **Next**.
8. On the SQL Server Setup page, specify the SQL Server instance where the databases are installed, and provide SQL credentials for the remote database. Click **Next**.

   You can optionally click **Test** to validate your connection with the database server.
9. On the Select Features page, select **AMP Proxy**. If you also want to install the Redirector, select **AMP Redirector Service**. Click **Next**.



10. On the AMP Service Configuration page, enter the web address of the Notification service, and then click **Next**. The recommendation is to use the internal IP address of the system where the Notification service is installed in the URL. This will avoid any issues with the name resolving to an IPV6 IP address instead of an IPV4 address. The Proxy is unable to connect to the Notification service when using an IPV6 address.

11. On the Configure AMP Proxy page, specify the AMP Proxy domain name and IP address, and then click **Next**. The domain name provided here should be the name that is accessible and resolvable by all agents.

    For configurations where the agents will be located outside your network, this address would be the external domain name registered for your environment. For configurations where the Agents are only located within your local network (LAN), the name can be the system name for the system where the Proxy is installed. The address that is provided for the Portal is the internal IP address for the system where the proxy installed.

12. On the AMP Redirector Service Configuration page, enter the Registration Service web address, and then click **Next**. The recommendation is to use the internal IP address of the system where the Registration service is installed in the URL. This will avoid any issues with the name resolving to an IPV6 IP address instead of an IPV4 address.

13. On the Services/Support Files page, enter the location for installing services and support files, and then click **Next**.

14. On the Machine Key File page, specify the full path and file name of the PortalKey.txt file that you copied to the server in Step 3, and then click **Next**.

    The installer checks the PortalKey.txt file. If the file contains a valid machine key, the installation continues.

    If there is a problem with the PortalKey.txt file, a "*values in the message key file are not correct*" message appears. Please check the file and try the installation again.

15. In the confirmation dialog box, click **Yes**.

- After the components are installed, a Component Status page appears. This page indicates which components have been installed and which components need to be installed before the system will be operational.
- The page also indicates if one of the components is not at the same versions as the other components and will still need to be upgraded. Components which are currently installed, but are not up to the current version, may show as missing.
- To save a copy of the Component Status information, enter a location for saving the file, and then click **Save**.

16. Click **Next**.

17. On the Portal Installation Successful page, click **Finish**.

3.1.4 (Recommended) Configure Windows authentication for database access

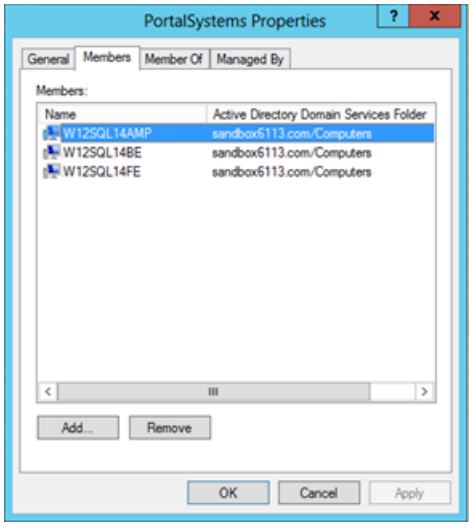
By default, Portal components in a distributed system use SQL Server authentication to access the database. We recommend configuring Windows authentication for database access.

When using Windows authentication for database access, Portal services should not run using the Local System account. A valid user with sysadmin permissions should be used for the services.

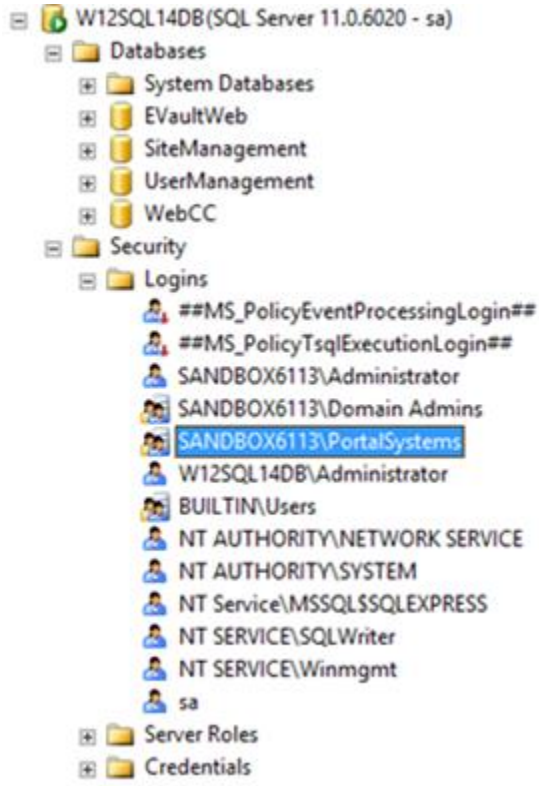
Prerequisite: Systems where Portal components are installed must all be members of the same domain.

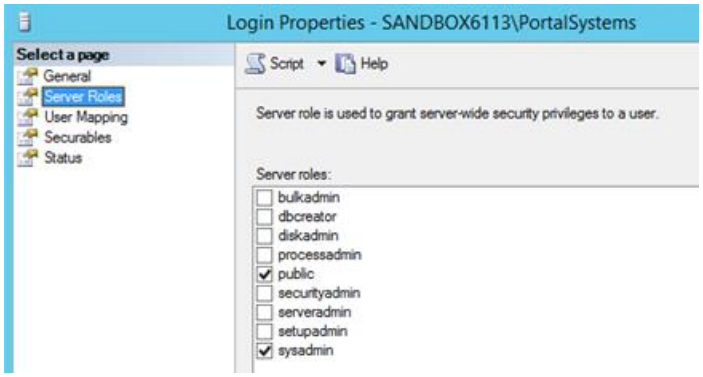
To configure Windows authentication for database access:

1. Install Portal using SQL Server authentication.
2. Create a domain group. Add accounts to the domain group for all systems where Portal components are installed. For example:



3. Add the group created in Step 2 as a Login to SQL Server, and add the sysadmin role to the group.





4. Check the account that is used for running each Portal service. Make sure that each Portal service is not running using the Local System account. When using Windows authentication for database access, Portal services should not run using the Local System account. Instead, choose another valid user with sysadmin permissions for each service.

5. In each configuration file listed in Configuration files with database connection strings, find each database connection string and replace the User ID and Password elements with: `Integrated Security=SSPI`

   For example, change the following database connection strings:

```
<add name="EVaultWeb" connectionString="Data
Source='SQLinstance';Database='EVaultWeb';User
ID='username';Password='password';Pooling=False"
providerName="System.Data.SqlClient" />

<add key="WebCC.Sql.Connection" value="Data
Source='SQLInstance';Database='WebCC';User
ID='user';Password='password'" />
```

To:

```
<add name="EVaultWeb" connectionString="Data
Source='SQLinstance';Database='EVaultWeb'; Integrated
Security=SSPI;Pooling=False" providerName="System.Data.SqlClient" />

<add key="WebCC.Sql.Connection" value="Data
Source='SQLInstance';Database='WebCC';Integrated Security=SSPI" />
```

Configuration files with database connection strings

Component	Configuration file
Back-end components	
Task Service	`C:\Program Files\`*`<application>`*`\Portal Services\TaskService\TaskService.exe.config`*
Notification Service	`C:\inetpub\Portal Services Website\Notification\web.config`
Registration Service	`C:\inetpub\Portal Services Website\Registration\web.config`
Front-end components	
Portal UI	`C:\inetpub\Portal Website\web.config`
Redirector	`C:\Program Files\`*`<application>`*`\Portal Services\AMP Redirector Service\RedirectorService.exe.config`*
Proxy	`C:\Program Files\`*`<application>`*`\Portal Services\AMP Proxy Service\AmpService.exe.config`*
Service Connector API	`C:\inetpub\Portal Services Website\Portal_Service_Connector\web.config`
Host Protect API	`C:\inetpub\Portal Services Website\Host_Protect\web.config`
API Task Scheduler	`C:\Program Files\`*`<application>`*`\Portal Services\API Scheduler\EVaultSDK.Scheduler.exe.config`*
Portal Task Scheduler	`C:\Program Files\`*`<application>`*`\Portal Services\Task Scheduler\EVault.Web.TaskScheduler.exe.config`*

* The *<application>* value is “OpenText Server Backup” for fresh Portal installs and “Carbonite Server Backup” for Portal instances that were upgraded from version 9.31 or earlier.

3.2 Install Portal on a single system

You can install all Portal components on a single server. However, this configuration is only suitable for small deployments (fewer than 500 Agents).

To install Portal on a single system:

1. Sign in as an administrator, and run the Portal installation kit.
2. On the Welcome page, click **Next**.
3. On the View Notes page, click **Next**.
4. On the License Agreement page, read the license agreement. Select **I accept the terms of the license agreement**, and then click **Next**.
5. On the SQL Server Setup page, choose the SQL Server instance where the databases will be installed. Specify the authentication method, and then click **Next**.

   We recommend using Window authentication for the database connection. To use Windows authentication, you must be logged in as a user with full access to the database server.

   (Optional) Click **Test Connection** to validate your connection with the database server.

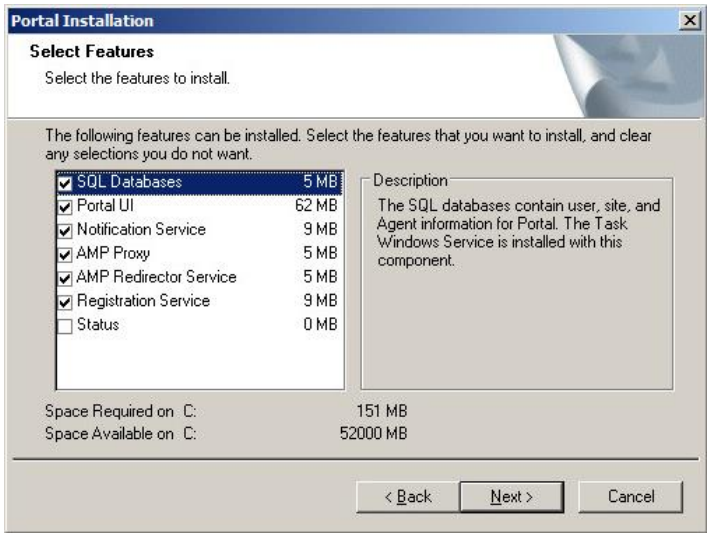
   Notes:

   - The SQL Server instance must have been installed with mixed mode authentication.
   - The SQL Server instance cannot contain existing EVaultWeb, WebCC, UserManagement, or SiteManagement databases.
   - If you want to install Portal with a remote SQL Server, install the sqlcmd utility from Microsoft on the machine where you are installing Portal. Otherwise, a “failure to create database” error might occur during the installation.
6. On the Select Features page, select the following items, and then click **Next**.

   - SQL Databases

   Note: The Task Service is installed with the SQL databases.

   - Portal UI
   - Notification Service
   - AMP Proxy
   - AMP Redirector Service
   - Registration Service



7. On the Language Selection page, select languages for displaying Portal text, and then click **Next**. In addition to the default English, you can select English (United Kingdom), French, German and Spanish.

   Note: When Portal is viewed in English (United Kingdom), times are shown in 24-hour clock format.

   If you do not install a language, you can add it later by rerunning the installation in Modify mode. You can also remove a language this way.

8. On the Domain Name page, specify the Portal domain name and port, and then click **Next**.

   On this page, you can provide the domain name for Portal, as well as the protocol to use (http/https). This specifies the address for users to connect to Portal.

   We highly recommend that you install Portal with the https protocol. For https, a signed certificate must be applied to the website where this application is installed. Make sure that the certificate matches the domain name that you are using for Portal, and import the certificate into IIS after the Portal installation is complete.

   Note: If a load balancer will handle https connections to the Portal UI, you must install Portal with the http protocol. For more information, see Install front-end system components.

   Note: Beginning in version 8.85, Portal uses SSL by default. While it is not recommended (unless a load balancer will handle https connections to the Portal UI), you can configure Portal to not use SSL. See Configure Portal to not use SSL.

   When configuring the system for external access, the domain name that is provided here should be the name which is registered on the internet for Portal. If the system is being set up before external access is configured, the application will only work after you successfully set up the domain name that has been provided here. If the domain name changes after installation, the installed components will need to be manually updated.

9. On the Portal – Select Installation and Log Paths page, specify the Portal installation location and Logs location, and then click **Next**.
10. On the Portal Service Connector – Location and Virtual Directory page, specify the following information, and then click **Next**:
    - Installation location
    - Log file location
    - Virtual Directory Name. Change this name if it will conflict with another already installed website/service.
11. On the Host Protect – Locations and Virtual Directory page, specify the following information, and then click **Next**:
    - Installation location
    - Log file location
    - Virtual Directory Name. Change this name if it will conflict with another already installed website/service.
12. On the API Scheduler Installation page, specify the following information, and then click **Next**:
    - Installation location
    - Log file location
13. On the Task Scheduler – Select Installation Path page, specify the Task Scheduler installation location and log file location, and then click **Next**.
14. On the Notification Service – Locations and Virtual Directory page, specify the following Notification service information, and then click **Next**:
    - Installation location
    - Log file location. For security reasons, the log files should not be under the same path where the Notification service is installed.
    - Virtual Directory Name. Change this name if it will conflict with another already installed website/service. If you change the virtual directory name, record it. You will need to enter it when installing the proxy.
15. On the Registration Service – Locations and Virtual Directory page, specify the following information, and then click **Next**:
    - Installation location
    - Log file location

- Virtual Directory Name. Change this name if it will conflict with another already installed website/service. If you change the virtual directory name, record it. You will need to enter it when installing the proxy.

16. On the AMP Proxy IP Configuration page, specify the AMP Proxy domain name and IP address, and then click **Next**. The domain name provided here should be the name that is accessible and resolvable by all agents.

    For configurations where the agents will be located outside your network, this address would be the external domain name registered for your environment. For configurations where the Agents are only located within your local network (LAN), the name can be the system name for the system where the Proxy is installed. The address that is provided for the Portal is the internal IP address for the system where the proxy installed.

17. On the Services/Support Files page, enter the location for installing services and support files, and then click **Next**.

18. In the confirmation dialog box, click **Yes**.

    After the components are installed, a Component Status page appears. This page indicates which components have been installed and which components need to be installed before the system will be operational.

    The page also indicates if one of the components is not at the same versions as the other components and will still need to be upgraded. Components which are currently installed, but are not up to the current version, may show as missing.

    To save a copy of the Component Status information, enter a location for saving the file, and then click **Save**.

19. Click **Next**.

20. On the Portal Installation Successful page, click **Finish**.

21. After Portal is installed, make a backup copy of the Portal Website web.config file (C:\inetpub\Portal Website\web.config, by default) and keep the backup copy somewhere safe. You might need this file when converting Portal from a single system to a two-server distributed system or recovering Portal after a disaster.

4 Manage the Portal AMP Proxy certificate

When you install Portal, a self-signed AMP Proxy certificate is generated for verifying connections between agents and Portal. We recommend replacing the self-signed certificate with an RSA certificate from an enterprise or commercial Certificate Authority (CA) **before** agents are registered to the Portal instance.

IMPORTANT: Recent agent versions check the public key of the AMP Proxy certificate when they try to connect to Portal. If the public key is different than when they first connected to Portal (i.e., when a new agent registered to Portal or an existing agent was upgraded to a version that checks the public key of the AMP Proxy certificate), the agents will stop connecting to Portal.

If you are not sure whether a Portal instance is using a self-signed or CA certificate, and to check the certificate validity period, see Check the Portal AMP Proxy certificate type and expiry date.

To replace a self-signed certificate with a CA signed certificate, see Replace the Portal AMP Proxy certificate.

To ensure that agents can connect to Portal after you obtain a new CA certificate, generate a Certificate Signing Request (CSR) with the same public key as the current certificate. See Generate a Certificate Signing Request with the same public key as the current certificate.

While it is not recommended, if you choose to use the self-signed AMP Proxy certificate that is generated when Portal is installed, you can extend the validity period of the self-signed certificate. See Extend the validity period of the self-signed Portal AMP Proxy certificate.

4.1 Check the Portal AMP Proxy certificate type and expiry date

This section describes how to check the Portal AMP Proxy certificate and determine:

- whether the certificate is self-signed or CA signed. We recommend replacing the self-signed certificate that is generated when you install Portal with an RSA certificate from an enterprise or commercial Certificate Authority (CA), **before** agents are registered to the Portal instance. See Replace the Portal AMP Proxy certificate.
- the validity period of the AMP Proxy certificate. If a CA certificate is expiring, you can generate a Certificate Signing Request with the same public key as the current certificate. If the self-signed certificate is expiring, see Extend the validity period of the self-signed Portal AMP Proxy certificate.

To check the Portal AMP Proxy certificate type and expiry date:

- On a computer where OpenSSL is installed, at a command prompt, navigate to the directory where OpenSSL is installed.
- Run the following command:

  ```
  openssl s_client -showcerts -connect PortalAddress:8086 | openssl
  x509 -noout -dates
  ```

  To check the AMP Proxy certificate instead of the Portal UI certificate, you must include the port number (8086) at the end of the Portal address.

  If the AMP Proxy certificate is the self-signed certificate that was installed with Portal, the command returns something like the following (where the certificate name is WebCC and the certificate is self-signed):

  ```
  depth=0 CN = WebCC, C = , O = , L = , ST = ,
  emailAddress =
  verify error:num=18:self signed certificate
  verify return:1
  depth=0 CN = WebCC, C = , O = , L = , ST = ,
  emailAddress =
  verify return:1
  read:errno=0
  notBefore=Feb  3 00:00:00 2021 GMT
  notAfter=May  8 00:00:00 2023 GMT
  ```

  If the certificate is from a certificate authority, the command returns something like:

  ```
  depth=1 C = Country, ST = State, L = City, O = Corporation
  Service Company, CN = Trusted Secure Certificate
  Authority 5
  verify error:num=20:unable to get local issuer
  certificate
  verify return:1
  depth=0 C = Country, postalCode = postalCode, ST = State, L
  = City, street = street, O = "company", OU = organization, CN
  = *.company.com
  verify return:1
  notBefore=Apr 30 00:00:00 2020 GMT
  notAfter=Apr 30 23:59:59 2022 GMT
  read:errno=0
  ```

  In each case, the “notAfter” value indicates when the certificate expires.

4.2 Replace the Portal AMP Proxy certificate

We recommend replacing the self-signed certificate that is generated when you install Portal with an RSA certificate from an enterprise or commercial Certificate Authority (CA), **before** agents are registered to the Portal instance.

IMPORTANT: If you replace the AMP Proxy certificate after agents are registered to the Portal instance, and the new certificate has a different public key, recent agent versions will stop connecting to Portal. This can occur beginning with Windows Agent 8.71, Linux Agent 8.63, AIX Agent 9.00, vSphere Recovery Agent 8.82 and Hyper-V Agent 9.10.

To prevent this issue, you can generate a Certificate Signing Request (CSR) with the same public key as the current certificate. You can then obtain and import a certificate with the same public key. See Generate a Certificate Signing Request with the same public key as the current certificate.

If agents stop connecting to Portal because the AMP Proxy certificate has changed, you must either:

- Replace the AMP Proxy certificate with the original certificate or another certificate with the same public key, and then restart all agents that are registered to Portal.
- Do the following:
    - Re-register Windows, Linux, AIX and vSphere Recovery agents to Portal.
    - Recover jobs and settings from Hyper-V agents that are not connecting to Portal.

To replace the self-signed AMP Proxy certificate that is generated when Portal is installed, you can use a Certificate Import tool that is provided with Portal. This tool can replace the current AMP Proxy certificate with an RSA certificate in .pem, .crt, or .pfx format.

You can use the same certificate for each AMP Proxy. The FQDN of the certificate does not have to match the FQDN of the AMP Proxy server.

When replacing a Portal AMP Proxy certificate, the Certificate Import tool backs up the existing AMP Proxy certificate in .pem format. If problems occur, you can use the tool to re-import the certificate from the .pem file. See Roll back to a previous Portal AMP Proxy certificate. We recommend backing up this certificate file to ensure that it can be restored.

To replace the Portal AMP Proxy certificate:

1. Obtain the RSA certificate file for the Portal instance in .pem, .pfx, or .crt format, and save the file on the machine where the Portal AMP Redirector is installed.

You can only import a certificate in .crt format if it has the same public key as the current AMP proxy certificate.

You can import a certificate in .pem or .pfx format if it has the same public key or a different public key than the current AMP proxy certificate.

2. On the machine where the Portal AMP Redirector is installed, log in as an administrator.

   If Portal was installed using Windows Authentication, log in as an administrator that has permission to access the master, model, Msdb and tempdb databases (DBOwner).

3. Open a command prompt and navigate to the …\AMP Redirector Service\Tools\AMP.Certificate.Import folder. By default, this folder is C:\Program Files\<*application*>\Portal Services\AMP Redirector Service\Tools\AMP.Certificate.Import, where <*application*> is “OpenText Server Backup” for fresh Portal installs and “Carbonite Server Backup” for Portal instances that were upgraded from version 9.31 or earlier.

4. Run the following command:

   `AMP.Certificate.Import.exe -t [Pem|Pfx|Certificate] -f` *`certificatePathandFile`* `[-p` *`pfxPassword`*`]`

   Where:

   - -t [Pem|Pfx|Certificate] specifies whether the certificate file being imported is in .pem, .pfx, or .crt format.

     If you are importing a certificate in .pfx format, you must include the -p *pfxPassword* parameter in the command. You can import a certificate in .pem or .pfx format if it has the same or a different public key than the current AMP proxy certificate.

     You can only import a certificate in .crt format if it has the same public key as the current AMP proxy certificate.

   - -f *certificatePathandFile* specifies the location and file name of the certificate file that you are importing.

   - If you are importing a certificate in .pfx format, -p *pfxPassword* specifies the password of the .pfx file that you are importing. The password is case-sensitive.

   For example, to replace the current Portal AMP.Proxy certificate using a certificate file named cert.pfx, you could run the following command:

   ```
   AMP.Certificate.Import.exe -t Pfx -f C:\cert.pfx -p
   password
   ```

If the new certificate is imported successfully, a “Certificate imported successfully” message appears, along with information about the certificate.

If the certificate is not imported successfully, an error message appears. For more information, see the log file that is saved in the directory where you ran the import tool. The log file is named AMP_certificate_import_*yyyy-mm-dd*.log, where *yyyy-mm-dd* represents the date when you ran the import tool.

The current AMP Proxy certificate is backed up in a .pem file in the folder where you ran the import tool. The backup file will be named backup_certificate_*yyyy-mm-dd-hh-mm-ss*.pem, where *yyyy-mm-dd-hh-mm-ss* represents the date and time when you replaced the certificate. You can roll back to this certificate if problems occur. See Roll back to a previous Portal AMP Proxy certificate.

5. After the new certificate has been successfully imported, restart the following Portal services:

   - AMP Proxy
   - AMP Redirector

   If Portal is installed as a distributed system, restart these services on every server where the services are installed.

6. Restart the OpenText Server Backup API Scheduler service.

   If Portal is installed as a distributed system, only restart the API Scheduler service on the server where it is running. The API Scheduler should only run on one Portal UI server.

7. Restart IIS (Internet Information Services). If Portal is installed as a distributed system, restart IIS on every server where Portal components are installed.

4.2.1 Roll back to a previous Portal AMP Proxy certificate

When you replace the AMP Proxy certificate in a Portal instance as described in Replace the Portal AMP Proxy certificate, the certificate that you are replacing is backed up in a .pem file in the folder where you run the import tool. You can roll back to this certificate if problems occur.

To roll back to a previous Portal AMP Proxy certificate:

1. Obtain the .pem file with the previous AMP Proxy certificate. The .pem file is named backup_certificate_*yyyy-mm-dd-hh-mm-ss*.pem, where *yyyy-mm-dd-hh-mm-ss* represents the date and time when you replaced the certificate.

   Initially, the .pem file is saved in the folder where you ran the import tool.

2. Import the .pem file as described in Replace the Portal AMP Proxy certificate.

For example, to roll back to a certificate in a file named backup_certificate_2022-03-26-11-24-35.pem, you could run the following command:

```
AMP.Certificate.Import.exe -t Pem -f
backup_certificate_2022-03-21-14-22-54.pem
```

Note: If the .pem file is in the …\AMP Redirector Service\Tools\AMP.Certificate.Import folder, you do not need to specify the path to the .pem file.

4.3 Generate a Certificate Signing Request with the same public key as the current certificate

If the public key of the Portal AMP Proxy certificate changes after recent agent versions are registered to the Portal instance, the agents will stop connecting to Portal. To prevent this issue, you can use a tool provided with Portal to generate a Certificate Signing Request (CSR) with the same public key as the current certificate. You can then submit the CSR to a Certificate Authority to obtain a new RSA certificate with the same public key.

You can use the same certificate for each AMP Proxy. The FQDN of the certificate does not have to match the FQDN of the AMP Proxy server.

To generate a Certificate Signing Request with the same public key as the current certificate:

1. On the machine where the Portal AMP Redirector is installed, log in as an administrator.

   If Portal was installed using Windows Authentication, log in as an administrator that has permission to access the master, model, Msdb and tempdb databases (DBOwner).

2. Open a command prompt and navigate to the …\AMP Redirector Service\Tools\GenerateSigningRequest folder. By default, this folder is C:\Program Files\<*application*>\Portal Services\AMP Redirector Service\Tools\AMP.Certificate.GenerateSigningRequest, where <*application*> is "OpenText Server Backup" for fresh Portal installs and "Carbonite Server Backup" for Portal instances that were upgraded from version 9.31 or earlier.

3. Run the following command:

   ```
   AMP.Certificate.GenerateSigningRequest.exe -n serverFQDN [-o
   organizationName]  -c countryCode -s stateOrRegion -l city -u
   division -f outputPathandFile
   ```

   Where:

   - -n *serverFQDN* specifies the fully-qualified domain name (FQDN) of the AMP Proxy (e.g., *.company.com or portal.company.com). The domain name provided here should be the name that is accessible and resolvable by all Agents.

- -o *organizationName* specifies the legal name of your organization. The name should not be abbreviated and should include suffixes such as Inc, Corp or LLC (e.g., Company Inc).
- -c *countryCode* specifies a two-letter ISO code for the country where your organization is located (e.g., US, GB).
- -s *stateOrRegion* specifies the state or region where your organization is located. The state or region name should not be abbreviated (e.g., California or Ontario).
- -l *city* specifies the city where your organization is located (e.g., Toronto or Mountain View).
- -u *division* specifies the division of your organization that is handling the certificate (e.g., IT Department). This parameter is optional.
- -f outputPathandFile

If a signing request is generated, a “signing request has been generated” message appears, followed by the certificate request. The certificate request is also saved to the specified file.

You can now provide the certificate request to a Certificate Authority to obtain an RSA certificate with the same public key as the original certificate. After obtaining the certificate, import it into the Portal instance. See Replace the Portal AMP Proxy certificate.

If a signing request is not generated, see the log file that is saved in the directory where you ran the Certificate Signing Request tool. The log file is named AMP_certificate_generate_signing_request_*yyyy-mm-dd*.log, where *yyyy-mm-dd* represents the date when you ran the tool.

4.4 Extend the validity period of the self-signed Portal AMP Proxy certificate

Although it is not recommended, if you choose to use the generated self-signed AMP Proxy certificate in a Portal instance, you can use a Certificate Renew tool provided with Portal to extend the certificate validity period for 824 days.

When extending the validity period of the self-signed certificate, the Certificate Renew tool backs up the existing AMP Proxy certificate in .pem format. If problems occur, you can use the Certificate Import tool to re-import the previous certificate from the .pem file. See Roll back to a previous Portal AMP Proxy certificate. We recommend backing up this certificate file to ensure that it can be restored, if required.

To extend the validity period of the self-signed Portal AMP Proxy certificate:

1. On the machine where the Portal AMP Redirector is installed, log in as an administrator.

   If Portal was installed using Windows Authentication, log in as an administrator that has permission to access the master, model, Msdb and tempdb databases (DBOwner).

2. Open a command prompt and navigate to the …\AMP Redirector Service\Tools\AMP.Certificate.Renew folder. By default, this folder is C:\Program Files\<*application*>\Portal Services\AMP Redirector Service\Tools\AMP.Certificate.Renew, where <*application*> is "OpenText Server Backup" for fresh Portal installs and "Carbonite Server Backup" for Portal instances that were upgraded from version 9.31 or earlier.

3. Run the following command:

   ```
   AMP.Certificate.Renew.exe
   ```

   The current Portal AMP Proxy certificate will be backed up in a .pem file in the folder where you are running the import tool. The backup file is named backup_certificate_*yyyy-mm-dd-hh-mm-ss*.pem, where *yyyy-mm-dd-hh-mm-ss* represents the date and time when you ran the command. You can roll back to this certificate if problems occur. See Roll back to a previous Portal AMP Proxy certificate.

   IMPORTANT: We recommend backing up this certificate file to ensure that it can be restored, if required.

   If the certificate validity is successfully extended, a "Certificate has been successfully updated in the database" message appears, followed by information about the certificate.

   If the certificate validity is not extended, see the log file that is saved in the directory where you ran the Certificate Renew tool. The log file is named AMP_certificate_renew_*yyyy-mm-dd*.log, where *yyyy-mm-dd* represents the date when you ran the tool.

4. After the certificate validity is successfully extended, restart the following Portal services:

   - AMP Proxy
   - AMP Redirector

   If Portal is installed as a distributed system, restart these services on every server where the services are installed.

5. Restart IIS (Internet Information Services). If Portal is installed as a distributed system, restart IIS on every server where Portal components are installed.

5 Integrate Portal with EVault Reports

Beginning in Portal 9.00, the Reports page appears in all Portal instances. In previous versions, the Reports page only appeared if Portal was integrated with Server Backup EVault Reports.

If Portal is not integrated with EVault Reports, the following reports are available on the Reports page:

- Backup Verification Report
- Daily Status Report
- Custom Command Report

If Portal is integrated with EVault Reports, additional reports with detailed information about customers' backups, restores and vault space usage are available on the Reports page in Portal.

To integrate Portal with EVault Reports, do the following:

- Enable Reports integration in Portal
- Associate customer short names with Portal sites

Note: To install EVault Reports, see the *EVault Reports Installation and Migration Guide*.

5.1 Enable Reports integration in Portal

To enable Reports integration in Portal:

1. Log in to Portal as a Super user.
2. On the navigation bar, click **Global Settings**.
3. Click the **Report Settings** tab.
4. On the Report Settings tab, select the **Enable Reports integration** check box.
5. In the **Connectivity** section, enter Reports database information and credentials.

   The specified user must have read permission to the Reports database.
6. In the **Token Manager Configuration** section, enter the URL for the EVault Reports Token Manager service.
7. In the **Notifications** section, enter an email address for sending a notification if a customer shortname is missing. **Customer short name** values (from the vault) must be associated with **Report Group Name** values (from Reports Manager).
8. Click **Save**.

Note: If the specified Reports settings are not correct, reports that require EVault Reports integration do not appear on the Reports page in Portal and an error message appears at the bottom of the page.

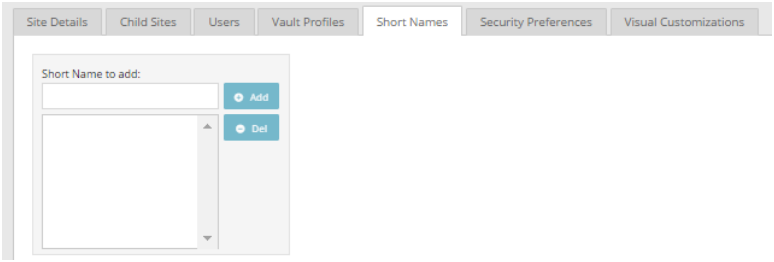
5.2 Associate customer short names with Portal sites

To allow your users to access reports, you must associate Customer short name values (from the vault) with Portal sites. If these values are not properly configured, users cannot access reports through Portal has been integrated. You can associate customer short names with sites using Portal.

For details about Customer short name values from the vault, see the *Director User Guide*.

To associate customer short names with a Portal site:

1. Log in to Portal as a Super user.
2. On the navigation bar, click **Sites**.
3. In the grid, open the site by clicking its row.
4. Click the **Short Names** tab.



5. In the **Short Name to add** box, type the short name (from the vault) to associate with the site.
6. Click **Add**.
7. Click **Save**.

Users in the site can now access reports that are associated with their customer short name.

6 Set up, enable or disable Portal features

6.1 Set up the data deletion feature

When the data deletion feature is set up in a Portal instance, an Admin user can delete a job or computer from Portal and request that backup data for the job or computer be deleted from all vaults. If the data deletion request is not canceled during a 72-hour waiting period, the deletion request is sent to vaults through API – Monitoring and the data is deleted from any standalone, Base or Active vault where the data is stored. Replication processes then delete the data from any associated Satellite or Passive vault.

The following steps are required to set up the data deletion feature:

- Portal must be registered to the same API – Monitoring instance as vaults where the backup data is stored. See the *Portal Administration Guide*.
- Data deletion email notifications must be set up. See Set up emailed reports and automatic emails and Customize data deletion emails.
- The Data Deletion feature must be enabled in Portal. See the *Portal Administration Guide*.

Note: In Portal versions earlier than 8.88, you had to enter machine keys in Portal configuration files when setting up the data deletion feature. Beginning in Portal 8.88, machine keys required for data deletion are populated in Portal configuration files when you install or upgrade Portal.

6.1.1 Configure Portal to use TLS 1.2 for vault data deletion requests

Beginning in Portal 9.10, Portal sends data deletion requests to API – Monitoring using the operating system's default TLS version. However, you can configure Portal to send data deletion requests using TLS 1.2.

To configure Portal to use TLS 1.2 for vault data deletion requests, run the following query on the Portal database server:

```
update [SiteManagement].[dbo].[SiteConfiguration] set
ConfigValue = 'tls12' where ConfigKey =
'PlatformApiMessageBusSecurityProtocol'
```

6.2 Enable or disable Portal features

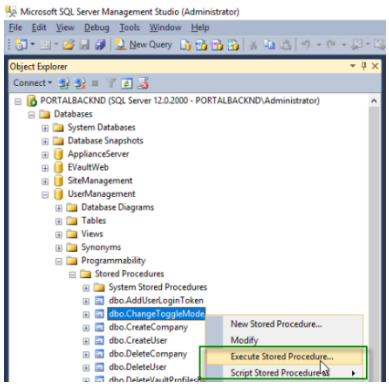
You can enable or disable some Portal features using a stored procedure in the Portal database. Using this procedure, you can:

- Enable a feature for all sites in the Portal instance.

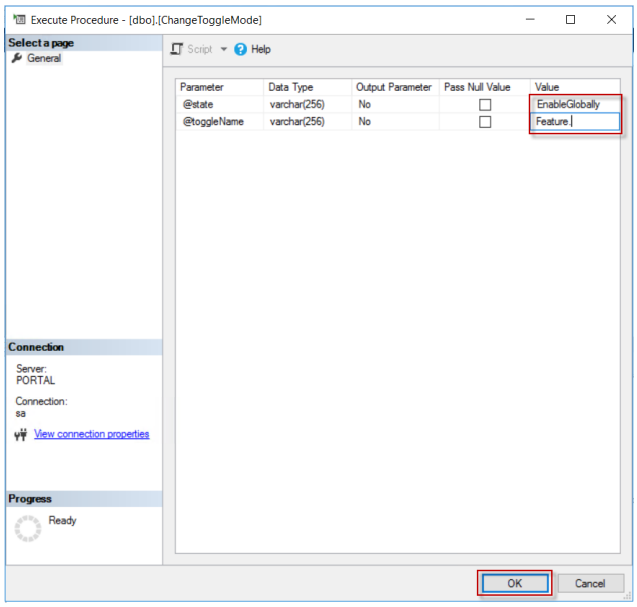
- Make a feature available in the Portal instance but leave it disabled for all sites. Super users or Admin users can then enable the feature for specific sites.
- Disable a feature for all sites in the Portal instance.

To enable or disable a Portal feature:

1. In SQL Server Management Studio (SSMS), connect to the Portal database server.
2. In the Object Explorer, go to **Databases** > **UserManagement** > **Programmability** > **Stored Procedures**.
3. Right-click **dbo.ChangeToggleMode** and select **Execute Stored Procedure** from the menu.



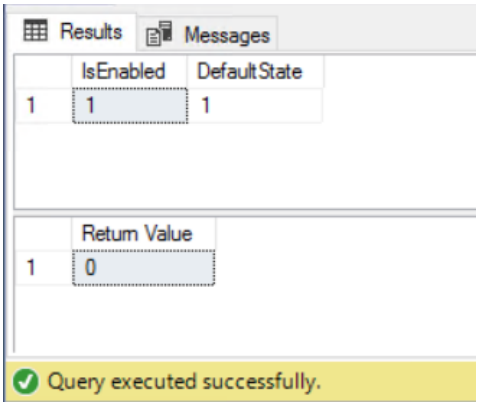
The Execute Procedure dialog box appears.



4. In the @state Value column, type one of the following values:
   - To enable the feature for all Portal sites, type: `EnableGlobally`
   - To make the feature available in Portal but leave it disabled in each site by default, type: `OptInPerCompany`
   - To disable the feature in the entire Portal instance, type: `Disabled`
5. In the @toggleName Value column, type the value for the feature you are enabling or disabling. For example, to enable or disable welcome emails, type: `Feature.WelcomeEmail`

   OpenText can provide other @toggleName values, as required.
6. Click **OK**.

   If the procedure runs successfully, the following values appear in the SSMS Results pane.



6.3 Enable the skipped rate feature

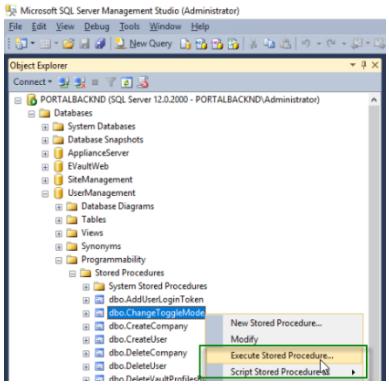
Beginning with Windows Agent 8.90, Linux Agent 8.90, AIX Agent 9.00 and vSphere Recovery Agent (VRA) 9.11, when an agent is backing up data to a Director 8.60 or later vault, users can schedule backup jobs to run multiple times per day, as often as hourly, by creating intra-daily schedules. When a backup job runs multiple times per day, backups are skipped in some cases to reduce schedule overload. For more information, see the *Portal User Guide*.

To help users monitor skipped backups, you can enable a skipped rate feature in Portal. When this feature is enabled, Portal shows the percentage of backups that were skipped for a job in the 48 hours before the last backup attempt. Users can click the skipped rate to view a 48-hour skipped rate history for the job.

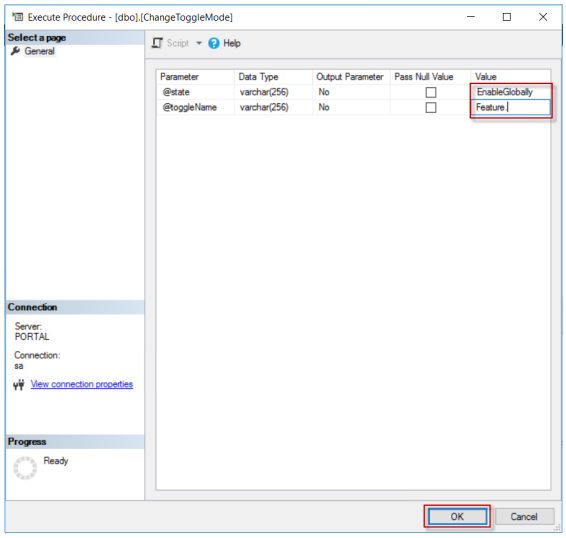
IMPORTANT: Before enabling the skipped rate feature, you must apply a hotfix for EV-71122 and EV-71491. This hotfix is available from your service provider.

To enable the skipped rate feature:

1. In SQL Server Management Studio (SSMS), connect to the Portal database server.
2. In the Object Explorer, go to **Databases** > **UserManagement** > **Programmability** > **Stored Procedures**.
3. Right-click **dbo.ChangeToggleMode** and select **Execute Stored Procedure** from the menu.

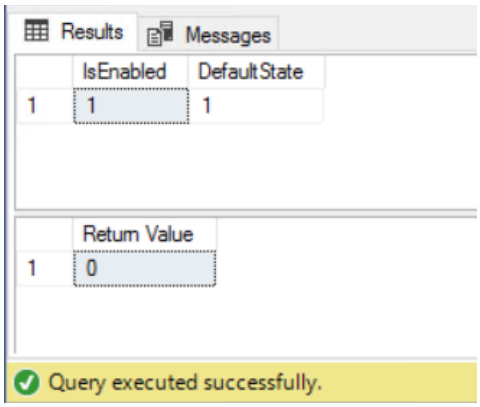


The Execute Procedure dialog box appears.



4. In the @state Value column, type: `EnableGlobally`
5. In the @toggleName Value column, type: `Feature.SkippedJobsRate`
6. Click **OK**.

   If the procedure runs successfully, the following values appear in the SSMS Results pane.



6.4 Enable or disable the Create New Site wizard

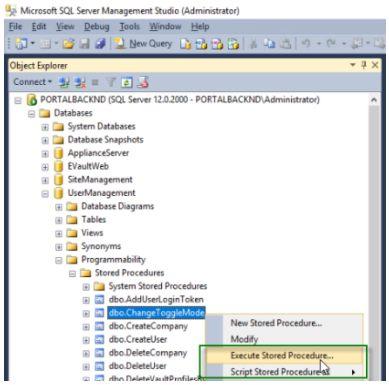
Beginning in Portal 9.50, you can enable a wizard that guides Admin users to create child sites with the following components needed for backing up servers:

- A registration-only user
- (Optional) An Admin user account
- A vault profile
- (Optional) Agent auto-configuration settings

By default, the Create New Site wizard is disabled. When disabled, the wizard does not appear when an Admin user clicks the “Create New Site” button on the Sites page, and the child site and other required components must be created separately.

To enable or disable the Create New Site wizard:

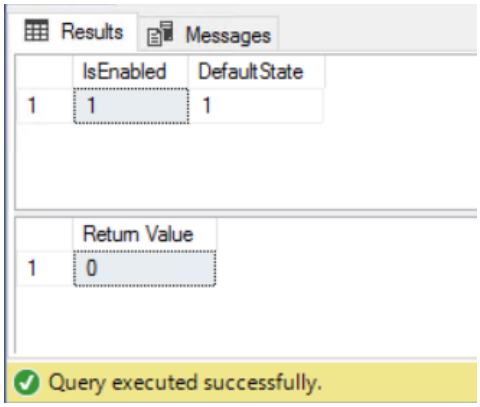
1. In SQL Server Management Studio (SSMS), connect to the Portal database server.
2. In the Object Explorer, go to **Databases** > **UserManagement** > **Programmability** > **Stored Procedures**.
3. Right-click **dbo.ChangeToggleMode** and select **Execute Stored Procedure** from the menu.



The Execute Procedure dialog box appears.

4. In the @state Value column, type one of the following values:
   - To enable the feature, type: `EnableGlobally`
   - To disable the feature, type: `Disabled`
5. In the @toggleName Value column, type: `Feature.SiteCreationWizard`
6. Click **OK**.

   If the procedure runs successfully, the following values appear in the SSMS Results pane.



6.5 Set up two-factor account verification

When two-factor account verification is set up in Portal, each user is prompted to provide a phone number for receiving account verification codes when they sign in to Portal. Users who set up two-factor account verification are prompted to enter a code periodically when they sign in to Portal and when they reset their passwords.

Beginning in Portal 9.10, a Super user can set up two-factor account verification by entering settings in the Portal UI. For more information, see the *Portal Administration Guide*. In previous Portal versions, two-factor account verification information was entered in Portal configuration files. If you upgrade to Portal 9.10, two-factor account verification settings are moved from configuration files to the Portal database and appear in the Portal UI.

Beginning in Portal 9.10, a Super user enables two-factor account verification on a Settings tab on the Global Settings page in Portal. See the *Portal Administration Guide*. In previous Portal versions, you had to run a UserManagement_DisableorEnableMultiFactorAuthentication.sql script on the SQL Server instance where Portal databases are installed.

6.5.1 Require users to set up two-factor account verification

Beginning in Portal 9.10, users in a Portal instance can be required to set up two-factor account verification. When two-factor account verification is required in a Portal instance, a **Skip this**

step option does not appear on the Portal page for setting up two-factor account verification and users who previously skipped setting up two-factor account verification are prompted to set it up.

IMPORTANT: Step 1 of this procedure is a test to see whether two-factor account verification is working in the Portal instance. If two-factor account verification is not working, **do not** perform steps 2-3 in this procedure. Otherwise, all users, including Super users, could be locked out of Portal.

To require users to set up two-factor account verification:

1. Check that two-factor account verification is working in the Portal instance by doing the following:

    a. Using a supported web browser, sign in to Portal as a Super user.

    If you are prompted to verify your account, enter your verification code and sign in.

    b. On the **Global Settings** page, click the **Settings** tab and then click the **Third Party MFA/2FA** tab. Check that settings appear on the tab.

    c. Click your user name at the top right of the Portal page and then click **Profile Settings**. In the Two-Factor Account Verification section, set up or change the phone number for receiving verification codes.

    d. Check your phone for an account verification code and enter the code in Portal.

    If you were able to set up or change your account verification settings and sign in to Portal, continue to the following steps.

    IMPORTANT: If you could not set up or change your account verification settings and sign in to Portal, **do not** perform steps 2 to 3 in this procedure until account verification is working in the Portal instance. Otherwise, all users, including Super users, could be locked out of Portal.

2. Require Portal users to set up two-factor account verification by doing the following:

    a. In SQL Server Management Studio (SSMS), connect to the Portal database server.

    b. In the Object Explorer, go to **Databases** > **UserManagement** > **Programmability** > **Stored Procedures**.

    c. Right-click **dbo.ChangeToggleMode** and select **Execute Stored Procedure** from the menu.

    d. In the Execute Procedure dialog box, do the following:

- In the @state **Value** column, type: `EnableGlobally`
- In the @toggleName **Value** column, type: `Feature.ForceMultiFactorAuthentication`

e. Click **OK**.

3. Require Portal users who previously skipped setting up two-factor account verification to set up two-factor account verification by doing the following:

   a. Obtain the UserManagement_ForceAllUsersToConfigureMfa.sql script from your software provider.

   b. Run the UserManagement_ForceAllUsersToConfigureMfa.sql script on the Portal database.

6.6 Display a new features list on the Sign In page

You can display a list of new features on the Portal Sign In page.

You can edit the list of new features, change the branding, and create a list in each Portal language. If you do not edit the new features list, it is OpenText-branded and in English. See Revise the new features list.

When the new features list includes the information and branding that you want, you can display it on the Portal Sign In page. See Display the new features list on the Sign In page.

If the new features list currently appears on the Sign In page and you want to hide it, see Hide the new features list on the Sign In page.

6.6.1 Revise the new features list

The new features list provided with Portal is OpenText-branded and in English. You can edit the information, change the branding, and create a list in each Portal language.

To revise the new features list:

1. On a Portal frontend system, go to C:\inetpub\Portal Website\assets\html and find the marketingbanner-en-US.html file.
2. Make a backup copy of the marketingbanner-en-US.html file.
3. In a text editor, open the marketingbanner-en-US.html file.
4. In the <body> section, find the feature sections. For each feature that you want to edit, change the featurename and featuredesc text.

For example, in the following feature section, you could change “Image Progress Bar” to another feature name and change “For a Windows Image job, the Process Details box shows the backup progress” to another feature description.

```
<div class="feature">
    <div class="featurename">
        Image Progress Bar
    </div>
    <div class="featuredesc">
        For a Windows Image job, the Process Details box shows
the backup progress.
    </div>
</div>
```

5. To replace OpenText branding in the list, do the following:

   a. Find the following lines:

      ```
      <div class="maincontent">
          <div class="heading1">
              OpenText Server Backup:
          </div>
      ```

      Replace “OpenText Server Backup” with your product name.

   b. To display the list on a white background instead of an image, find the following lines:

      ```
      background: url("../images/marketingbanner1.png") no-repeat
      center center fixed;
          background-size: cover;
      ```

      Comment out the lines by adding <!-- at the start of the first line and --> at the end of the second line. The resulting lines are:

      ```
      <!--   background: url("../images/marketingbanner1.png")
      no-repeat center center fixed;
          background-size: cover; -->
      ```

      Note: Alternatively, to show a different background image instead of a white background, make a backup copy of the C:\inetpub\Portal Website\assets\images\marketingbanner1.png file. Replace the image in the marketingbanner1.png file and then save the file.

   c. To replace the link for the “Learn More” button, find the following line:

      ```
      <a
      href="https://www.youtube.com/watch?v=xQ5w8kLYYzo&list=PLcPZG0
      JelebMafnMPZF-skbXJOvm49ptk" class="btn" target="_blank">Learn
      More</a>
      ```

Replace `https://www.youtube.com/watch?v=xQ5w8kLYYzo&list=PLcPZG0JelebMafnMPZF-skbXJOvm49ptk` with a link to another website or video.

6. Save the marketingbanner-en-US.html file.
7. To create a new features list in another Portal language, do the following:
   a. Make a copy of the marketingbanner-en-US.html file in C:\inetpub\Portal Website\assets\html. Name the file according to its language:

Language	Filename
French	marketingbanner-fr-FR.html
Spanish	marketingbanner-es-ES.html
German	marketingbanner-de-DE.html

   b. In a text editor, open the file and replace English text with text in the appropriate language.
   c. Repeat steps a and b for each Portal language.

   Note: If no html file is available for a Portal language, the new features list will appear in English when a user views the Sign in page in that language.
8. If the Portal UI is running on more than one server, copy the marketingbanner-en-US.html file and any files created in Step 7 to C:\inetpub\Portal Website\assets\html on each Portal UI server.
9. Create backup copies of the marketingbanner-en-US.html file and any files created in Step 7 and keep them somewhere safe.

6.6.2 Display the new features list on the Sign In page

By default, the new features list does not appear on the Sign In page.

To display the new features list on the Sign In page:

1. In SQL Server Management Studio, connect to the Portal database instance.
2. In the Object Explorer, go to **Databases** > **EVaultWeb** > **Programmability** > **Stored Procedures**.
3. Right-click **dbo.EnableFeature** and select **Execute Stored Procedure** from the menu.
4. In the Execute Procedure dialog box, in the @featureid row, type **25** in the Value column.
5. Click **OK**.

6.6.3 Hide the new features list on the Sign In page

If the new features list is displayed on the Sign In page, you can hide the list.

To hide the new features list on the Sign In Page:

1. In SQL Server Management Studio, connect to the Portal database instance.
2. In the Object Explorer, go to **Databases** > **EVaultWeb** > **Programmability** > **Stored Procedures**.
3. Right-click **dbo.DisableFeature** and select **Execute Stored Procedure** from the menu.
4. In the Execute Procedure dialog box, in the @featureid row, type **25** in the Value column.
5. Click **OK**.

7 Set up emailed reports and automatic emails

Portal uses an SMTP server to send automatic emails, such as welcome emails and backup notifications, and emailed reports. Some automatic emails can also be sent using Amazon Web Services (AWS) although this is not recommended in most cases.

Beginning in Portal 9.10, a Super user can enter SMTP server information and other email settings in the Portal UI. For more information, see the *Portal Administration Guide*. In previous Portal versions, email settings were entered in Portal configuration files. If you upgrade a Portal instance to version 9.10, email settings are moved from configuration files to the Portal database and appear in the Portal UI.

You can disable or enable welcome emails in a Portal instance. See Enable or disable Portal features.

You can also customize email templates for automatic emails, such as welcome emails and backup notifications, to include your organization's text and branding. See Customize automatic emails.

Reports that are emailed from Portal are customized using the site's logo, color, and company text. See the *Portal Administration Guide*.

7.1 Customize automatic emails

The following table lists and describes emails that Portal can send automatically, and indicates whether the emails are OpenText-branded or not branded (i.e., have no company logos or text) by default. Links to email customization instructions are provided for each type of email.

Note: Automatic emails are OpenText-branded beginning in Portal 9.4. In previous versions, automatic emails were Carbonite-branded.

Note: To customize emailed reports, see the *Portal Administration Guide*. Emailed reports include the logo, color, and company text specified for a site in Portal.

Automatic email	**Description**	**Default branding**	**Customization instructions**
Welcome (for setting initial passwords)	New users can receive "welcome" emails with links for setting their Portal passwords. After setting their passwords, users receive confirmation emails. Welcome emails are available beginning in Portal 8.89. To enable welcome emails in a Portal instance, see Set up emailed reports and automatic emails.	OpenText-branded; no logo	Customize welcome emails for setting Portal passwords

Automatic email	Description	Default branding	Customization instructions
Password reset	Users receive password reset emails after they click "Forgot my password" on the Portal sign-in page. After resetting their passwords, users receive confirmation emails.	OpenText-branded; no logo	Customize password reset emails
Backup notifications	Admin users and email addresses specified for child sites can receive centrally-configured notifications when backups finish or fail on Windows systems with Agent version 8.0 or later, Linux systems with Agent version 8.10a or later, AIX systems with Agent version 9.00 or later, and vSphere environments with vSphere Recovery Agent 8.40 or later. Backup notification emails are also sent when backups are canceled, deferred, missed or skips, or when potential ransomware threats are detected during a backup. *Note:* Beginning in Portal 9.10, a Super user enables centrally-configured backup email notifications on a Settings tab on the Global Settings page in Portal. See the *Portal Administration Guide*. In previous Portal versions, you had to run an EnableUserNotification.sql script on the SQL Server instance where Portal databases are installed.	OpenText-branded; no logo	Customize backup notification emails
Job encryption password change	Admin users and email addresses specified for child sites can receive emails when job encryption passwords change in their sites. Super users specify whether Admin users can receive encryption password change email notifications.	No branding	Customize emails for encryption password changes
Data deletion	Super users and Admin users in sites can receive emails when vault data deletions are scheduled or canceled. Vault administrators can receive email notifications when scheduled data deletions fail or require attention. The vault administrator's email address is specified in Portal.	No branding	Customize data deletion emails
Agent auto upgrade	Admin users receive email notifications when new agent auto upgrade installers are available in Portal. Super users and admin users receive email notifications when a computer needs to be restarted after an automatic upgrade.	No branding	Customize agent auto upgrade emails

7.1.1 Customize welcome emails for setting Portal passwords

If welcome emails are enabled in your Portal instance (see Enable or disable Portal features), you can customize welcome emails for new users to include your organization's text and branding. Welcome emails, which include links for setting initial Portal passwords, are available beginning in Portal 8.89. After setting their passwords, users receive confirmation emails.

If you do not customize the welcome email, new users receive an OpenText-branded email that asks them to set their Portal passwords. The subject line of the email is “Set your OpenText Server Backup password”.

If you do not customize the confirmation email, users receive an OpenText-branded email after setting a password. The subject line of the email is “Your login password has been set for OpenText Server Backup”.

To customize welcome emails for setting Portal passwords:

1. Find the BrandedTemplates.zip file in the …\Host_Protect\bin\EmailTemplates folder (C:\inetpub\Portal Services Website\Host_Protect\bin\EmailTemplates, by default).

   The BrandedTemplates.zip file contains many email templates and subject lines, including Welcome email templates and subject lines.
2. Extract the following files from the BrandedTemplates.zip file:

   - NewUserPasswordSetConfirmation.html
   - NewUserPasswordSetConfirmationSubject.txt
   - NewUserPasswordSetRequest.html
   - NewUserPasswordSetRequestSubject.txt

   Do not extract these files into the EmailTemplates folder (C:\inetpub\Portal Services Website\Host_Protect\bin\EmailTemplates, by default) before you customize the files.
3. To change the text or appearance of the Welcome email, edit the NewUserPasswordSetRequest.html file.

   To include an image in the email, host the image on a website or save the image in Portal Website\assets\images (C:\inetpub\Portal Website\assets images, by default). In the NewUserPasswordSetRequest.html file, remove the comment markings (<!-- and -->) from the following lines and edit the image link and information:

   ```
   <!--<a href="https://www.evault.com/" target="_blank">
      <img alt="Carbonite Server Backup" border="0"
   src="https://get.carbonite.com/rs/261-MDM-758/images/logo_carb-
   gry_300W.png" style="display: block !important; width: 100%;
   max-width: 160px; height: auto;" width="160"/>
       </a>-->
   ```

   Note: If Portal is hosted on a web farm and you save the logo image file locally, you must save the image file on every UI node in the farm.
4. To change the subject line of the Welcome email, edit the NewUserPasswordSetRequestSubject.txt file.

5. To change the text or appearance of the password set confirmation email, edit the NewUserPasswordSetConfirmation.html file.

   To include an image in the email, host the image on a website or save the image in Portal Website\assets\images (C:\inetpub\Portal Website\assets images, by default). In the NewUserPasswordSetConfirmation.html file, remove the comment markings (<!-- and -->) from the following lines and edit the image link and information:

   ```
   <!--<a href="https://www.evault.com/" target="_blank">
      <img alt="Carbonite Server Backup" border="0"
   src="https://get.carbonite.com/rs/261-MDM-758/images/logo_carb-
   gry_300W.png" style="display: block !important; width: 100%;
   max-width: 160px; height: auto;" width="160"/>
       </a>-->
   ```

   Note: If Portal is hosted on a web farm and you save the logo image file locally, you must save the image file on every UI node in the farm.

6. To change the subject line of the password set confirmation email, edit the NewUserPasswordSetConfirmationSubject.txt file.

7. Save the edited .html and .txt files in the following folders:

   - …\Host_Protect\bin\EmailTemplates (C:\inetpub\Portal Services Website\Host_Protect\bin\EmailTemplates, by default)
   - …\Portal Service Connector\bin\EmailTemplates (in C:\inetpub\Portal Services Website\Portal_Service_Connector\bin\EmailTemplates, by default).

8. By default, the following Support phone number appears in password set confirmation emails: 1-866-855-9555. To change the Support phone number, see Change the Support phone number in password-related emails.

7.1.2 Customize password reset emails

You can customize password reset emails to include your organization's text and branding.

If you do not customize password reset emails, users receive an OpenText-branded email after submitting password reset requests through Portal. The subject line of the email is "OpenText Server Backup password reset request".

Note: By default, the link in a password reset email is valid for 24 hours. You can change the link expiration time by running a script on the SQL Server instance where Portal databases are installed. To obtain this script, please contact Support.

If you do not customize password reset emails, a user receives an OpenText-branded email after resetting a password. The subject line of the email is “Your OpenText Server Backup password has been reset”.

To customize password reset emails:

1. Find the BrandedTemplates.zip file in the …\Host_Protect\bin\EmailTemplates folder (C:\inetpub\Portal Services Website\Host_Protect\bin\EmailTemplates, by default).

   The BrandedTemplates.zip file contains many email templates and subject lines, including OpenText-branded password reset email templates and subject lines.
2. Extract the following files from the BrandedTemplates.zip file:

   - PasswordResetConfirmation.html
   - PasswordResetConfirmationSubject.txt
   - PasswordResetRequest.html
   - PasswordResetRequestSubject.txt

   Do not extract these files into the EmailTemplates folder (C:\inetpub\Portal Services Website\Host_Protect\bin\EmailTemplates, by default) before you customize the files, or users will receive OpenText-branded emails.
3. To change the text or appearance of the Password Reset Request email, edit the PasswordResetRequest.html file.

   To include an image in the email, host the image on a website or save the image in Portal Website\assets\images (C:\inetpub\Portal Website\assets images, by default). In the PasswordResetConfirmation.html file, remove the comment markings (<!-- and -->) from the following lines and edit the image link and information:

   ```
   <!--<a href="https://www.evault.com/" target="_blank">
       <img alt="Carbonite Server Backup" border="0"
   src="https://get.carbonite.com/rs/261-MDM-758/images/logo_carb-
   gry_300W.png" style="display: block !important; width: 100%; max-
   width: 160px; height: auto;" width="160"/>
       </a>-->
   ```

   Note: If Portal is hosted on a web farm and you save the logo image file locally, you must save the image file on every UI node in the farm.

   If you do not edit the PasswordResetRequest.html file, users receive the following email after a password reset request.
4. To change the subject line of the Password Reset Request email, edit the PasswordResetRequestSubject.txt file.

If you do not edit the PasswordResetRequestSubject.txt file, the Password Reset Request email subject line is “OpenText Server Backup password reset request”.

5. To change the text or appearance of the Password Reset Confirmation email, edit the PasswordResetConfirmation.html file.

   To include an image in the email, host the image on a website or save the image in Portal Website\assets\images (C:\inetpub\Portal Website\assets images, by default). In the PasswordResetConfirmation.html file, remove the comment markings (<!-- and -->) from the following lines and edit the image link and information:

   ```
   <!--<a href="https://www.evault.com/" target="_blank">
       <img alt="Carbonite Server Backup" border="0"
   src="https://get.carbonite.com/rs/261-MDM-758/images/logo_carb-
   gry_300W.png " style="display: block !important; width: 100%; max-
   width: 160px; height: auto;" width="160" />
       </a>-->
   ```

   If you do not edit the PasswordResetConfirmation.html file, users receive an OpenText Server Backup email after a password reset.

6. To change the subject line of the Password Reset Confirmation email, edit the PasswordResetConfirmationSubject.txt file.

   If you do not edit the PasswordResetConfirmationSubject.txt file, the Password Reset Confirmation email subject line is “Your OpenText Server Backup password has been reset”.

7. Save the edited .html and .txt files in the EmailTemplates folder (C:\inetpub\Portal Services Website\Host_Protect\bin\EmailTemplates, by default).

   If you do not save the files in the EmailTemplates folder, users will receive unbranded emails.

8. By default, the following Support phone number appears in password reset emails: 1-866-855-9555. To change the Support phone number, see Change the Support phone number in password-related emails.

7.1.3 Change the Support phone number in password-related emails

Users receive automatic emails when they want to reset their Portal passwords and after they set or reset their passwords.

By default, the following Support phone number appears in these password-related emails: 1-866-855-9555. You can specify a different phone number for contacting Support.

To change the Support phone number in password-related emails:

1. In a text editor, open the web.config file for the Host Protect Service (C:\inetpub\Portal Services Website\Host_Protect\web.config, by default).

Find the following line:

```
<add key="SupportTelephoneNumber" value="1-866-855-9555" />
```

Replace 1-866-855-9555 with the Support number that you want to include in emails. The resulting line will be something like:

```
<add key="SupportTelephoneNumber" value="1-866-555-0101" />
```

Save the web.config file.

2. In a text editor, open the web.config file for the Portal Service Connector (C:\inetpub\Portal Services Website\Portal_Service_Connector\web.config, by default)

   Find the following line:

   ```
   <add key="SupportTelephoneNumber" value="1-866-855-9555" />
   ```

   Replace 1-866-855-9555 with the Support number that you want to include in emails. The resulting line will be something like:

   ```
   <add key="SupportTelephoneNumber" value="1-866-555-0101" />
   ```

   Save the web.config file.

7.1.4 Customize backup notification emails

You can customize backup notification emails to include your organization's text and branding. These notification emails can be sent for Windows systems where Agent version 8.0 or later is installed, Linux systems where Agent version 8.10a or later is installed, and vSphere environments protected by vSphere Recovery Agent 8.40 or later. Backup notification emails are also sent when backups are canceled, deferred, missed or skips, or when potential ransomware threats are detected during a backup.

Beginning in Portal 8.89, backup notification emails for a child site can be sent in any language that is available in the Portal instance.

Note: Email notifications selected in Admin users' profile settings are only supported in English.

IMPORTANT: In previous Portal versions, we described how to customize backup notification emails by editing the email template. We now recommend adding values in a configuration file instead of editing templates. This ensures that custom values appear in the emails in any language.

If you do not customize backup notification emails, Admin users receive OpenText-branded backup notification emails.

To customize backup notification emails:

1. On the server where the Portal UI is installed, go to the …Portal Services\API Scheduler folder. For fresh installs of this Portal version, the default location is C:\Program Files\OpenText Server Backup\Portal Services\API Scheduler.
2. In a text editor, open the EVaultSDK.Scheduler.exe.config file from the …Portal Services\API Scheduler folder.
3. Find the <appSettings> configuration element.
4. In the <appSettings> element, find the following line:

   ```
   <add key="PortalHostName" value="" />
   ```

   In the value quotation marks, type the Portal website address that will be included in backup notification emails.
5. In the <appSettings> element, after the `<add key="PortalHostName" value="" />` line, type the following lines:

   ```
   <add key="productName" value="yourProductName" />
   <add key="LogoLinkUrl" value="logoLinkURL" />
   <add key="LogoAlt" value="logoAltText" />
   <add key="LogoUrl" value="logoURL" />
   <add key="ServiceProviderName" value="serviceProviderName" />
   <add key="ServiceProviderLegalName" value="serviceProviderLegalName" />
   <add key="ServiceProviderAddress" value="serviceProviderAddress" />
   <add key="PrivacyPageUrl" value="privacyPageURL" />
   ```

   Where:

   - *yourProductName* is the server backup product name that will appear in backup notification email subject lines and text.
   - *logoLinkURL* is the URL accessed when someone clicks the logo in backup notification emails.
   - *logoAltText* is the alt text for the logo in backup notification emails.
   - *logoURL* is the link to the logo that will appear in backup notification emails.

     IMPORTANT: To display the logo in backup notification emails, you must also edit the email templates (e.g., BACKUP_COMPLETED.html). By default, the templates are located in language subfolders in C:\Program Files\<*application*>\Portal Services\API Scheduler\UserNotifications\Templates\ where <*application*> is “OpenText Server Backup” for fresh Portal installs and “Carbonite Server Backup” for Portal instances that were upgraded from version 9.31 or earlier. In each template, remove the comment markings (<!-- and -->) from the following lines:

```
<!--<a href="##LogoLinkUrl##" target="_blank">

     <img alt="##AltLogoText##" border="0" src="##LogoUrl##"
style="display: block !important; width: 100%; max-width:
160px; height: auto;" width="160"/>

    </a>-->
```

- *serviceProviderName* is the service provider name that will appear in backup notification emails.
- *serviceProviderLegalName* is the service provider legal name that will appear in backup notification email footers.
- *serviceProviderAddress* is the service provider's address that will appear in backup notification email footers.
- *privacyPageURL* is the URL for the service provider's privacy policy.

6. Save the EVaultSDK.Scheduler.exe.config file.
7. Restart the OpenText Server Backup API Scheduler service.

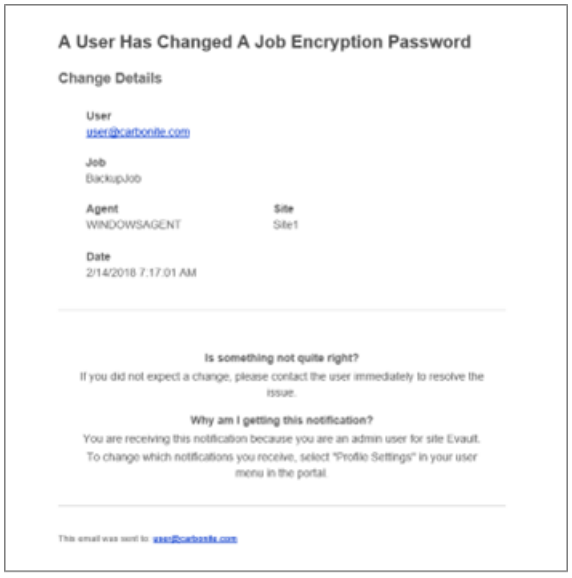
   Note: In a web farm, the API Scheduler service should only run on one Portal UI server.

7.1.5 Customize emails for encryption password changes

You can customize emails for encryption password changes to include your organization's text and branding. Beginning in Portal 8.89, encryption password change emails for a child site can be sent in any language that is available in the Portal instance.

Note: Email notifications selected in Admin users' profile settings are only sent in English.

If you do not customize encryption password change emails, users receive unbranded emails after an encryption password change in Portal, as shown in the following example in English. The subject line of the email in English is "Portal Job Encryption Password Change".


A User Has Changed A Job Encryption Password

Change Details

User
user@carbonite.com

Job
BackupJob

Agent
WINDOWSAGENT

Site
Site1

Date
2/14/2018 7:17:01 AM

Is something not quite right?
If you did not expect a change, please contact the user immediately to resolve the issue.

Why am I getting this notification?
You are receiving this notification because you are an admin user for site Evault. To change which notifications you receive, select "Profile Settings" in your user menu in the portal.

This email was sent to: user@carbonite.com

To customize emails for encryption password changes:

1. Go to the following folder: …\Portal_Service_Connector\bin\JobEncryption\Templates (C:\inetpub\Portal Services Website\Portal_Service_Connector\bin\JobEncryption\Templates, by default).

   This folder contains a subfolder for each language that is available in the Portal instance. Subfolders can include de-DE (German), en-GB (UK English), en-US (American English), es-ES (Spanish) and fr-FR (French).

   Each subfolder contains two files for the specified language:

   - JobEncryptionPasswordChangeSubject.txt — Contains the subject line for encryption password change notification emails.
   - JobEncryptionPasswordChange.html — Template for encryption password change notification emails.

2. To change the subject line of encryption password change notification emails in a certain language, edit the JobEncryptionPasswordChangeSubject.txt file in the appropriate language folder.

3. To change the text or appearance of encryption password change notification emails, do the following in each language subfolder:

   a. Make a copy of the JobEncryptionPasswordChange.html file. Edit this copied email template file to change the email text and/or appearance.

      To include an image in the email, host the image on a website or save the image in Portal Website\assets\images (C:\inetpub\Portal Website\assets\images, by default), and include a link in the html file.

Note: If Portal is hosted on a web farm, and you save the logo image file locally, you must save the image file on every UI node in the farm.

b. When satisfied with the edited email template, rename the original JobEncryptionPasswordChange.html file so that it will not be used as the email template. For example, you could change the file name to JobEncryptionPasswordChange-original.html.

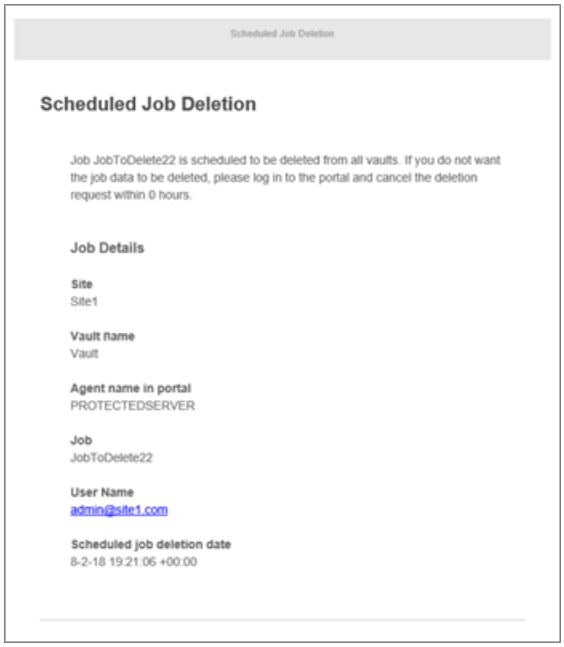
c. Rename the edited email template file to JobEncryptionPasswordChange.html. Encryption password change notification emails will then use this template.

d. Make a backup copy of the edited email template file so that it will not be overwritten during future Portal upgrades.

7.1.6 Customize data deletion emails

You can customize the emails that Super users and Admin users in sites receive when vault data deletions are scheduled, canceled or have problems. Emails are sent for job data deletions (feature added in Portal 8.6) and computer data deletions (feature added in Portal 8.8).

If you do not customize data deletion emails, users receive unbranded emails such as the following:



To customize emails for scheduled and canceled data deletions:

1. If you customized job data deletion emails in Portal 8.6 and did not previously rename the email files, rename the data deletion email files in the following locations as described in the table below:

- …\Portal_Service_Connector\bin\EmailTemplates folder (by default, C:\inetpub\Portal Services Website\Portal_Service_Connector\bin\EmailTemplates)
- …\Portal Services\API Scheduler\EmailTemplates (by default, C:\Program Files\<*application*>\Portal Services\API Scheduler\EmailTemplates, where <*application*> is "OpenText Server Backup" for fresh Portal installs and "Carbonite Server Backup" for Portal instances that were upgraded from version 9.31 or earlier)

Original File Name	**New File Name**
ScheduledDeletionSubject.txt	ScheduledJobDeletionSubject.txt
ScheduledDeletion.html	ScheduledJobDeletion.html
ScheduledDeletionCanceledSubject.txt	ScheduledJobDeletionCanceledSubject.txt
ScheduledDeletionCanceled.html	ScheduledJobDeletionCanceled.html
ScheduledDeletionAttentionSubject.txt	ScheduledJobDeletionAttentionSubject.txt
ScheduledDeletionAttention.html	ScheduledJobDeletionAttention.html
ScheduledDeletionFailureSubject.txt	ScheduledJobDeletionFailureSubject.txt
ScheduledDeletionFailure.html	ScheduledJobDeletionFailure.html
ScheduledDeletionNotSupportedSubject.txt	ScheduledJobDeletionNotSupportedSubject.txt
ScheduledDeletionNotSupported.html	ScheduledJobDeletionNotSupported.html

2. Find the BrandedTemplates.zip file in the …\Host_Protect\bin\EmailTemplates (C:\inetpub\Portal Services Website\Host_Protect\bin\EmailTemplates, by default).

   The BrandedTemplates.zip file contains email templates and subject lines for computer and job data deletions and for other Portal features.

3. Extract data deletion email files from the BrandedTemplates.zip file so that you can customize them. The email files are listed and described in the following table.

   Do not extract the files into a Portal Services or Portal Services Website subfolder or users might receive the emails before you finish customizing them.

   IMPORTANT: If you customized job data deletion emails in Portal 8.6, you might not want to extract and customize the job deletion email files. Instead, you can use the previously-customized emails (discussed in Step 1). Some job data deletion emails were updated in Portal 8.8, so you might want to use the new templates and subject lines.

Data Deletion Email Type	**File**	**Description**
Job deletion	ScheduledJobDeletionSubject.txt	Subject line for the email sent when someone schedules a job data deletion.

Data Deletion Email Type	File	Description
	ScheduledJobDeletion.html	Template for the email sent when someone schedules a job data deletion.
	ScheduledJobDeletionCanceledSubject.txt	Subject line for the email sent when someone cancels a scheduled job data deletion.
	ScheduledJobDeletionCanceled.html	Template for the email sent when someone cancels a scheduled job data deletion.
	ScheduledJobDeletionAttentionSubject.txt	Subject line for the email sent when a job data deletion request needs attention.
	ScheduledJobDeletionAttention.html	Template for the email sent when a job data deletion request needs attention.
	ScheduledJobDeletionFailureSubject.txt	Subject line for the email sent when a job data deletion request has failed.
	ScheduledJobDeletionFailure.html	Template for the email sent when a job data deletion request has failed.
	ScheduledJobDeletionNotSupportedSubject.txt	Subject line for the email sent when a job data deletion request is not supported by the vault.
	ScheduledJobDeletionNotSupported.html	Template for the email sent when a job deletion request is not supported by the vault.
Computer deletion	ScheduledComputerDeletionSubject.txt	Subject line for the email sent when someone schedules a computer data deletion.
	ScheduledComputerDeletion.html	Template for the email sent when someone schedules a computer data deletion.
	ScheduledComputerDeletionCanceledSubject.txt	Subject line for the email sent when someone cancels a scheduled computer data deletion.

Data Deletion Email Type	File	Description
	ScheduledComputerDeletionCanceled.html	Template for the email sent when someone cancels a scheduled computer data deletion.
	ScheduledComputerDeletionAttentionSubject.txt	Subject line for the email sent when a computer data deletion request needs attention.
	ScheduledComputerDeletionAttention.html	Template for the email sent when a computer data deletion request needs attention.
	ScheduledComputerDeletionFailureSubject.txt	Subject line for the email sent when a computer data deletion request has failed.
	ScheduledComputerDeletionFailure.html	Template for the email sent when a computer data deletion request has failed.
	ScheduledComputerDeletionNotSupportedSubject.txt	Subject line for the email sent when a computer data deletion request is not supported by the vault.
	ScheduledComputerDeletionNotSupported.html	Template for the email sent when a computer deletion request is not supported by the vault.

4. To change the subject line of data deletion notification emails, edit the text files listed in the table in Step 3.

5. To change the text or appearance of data deletion notification emails, edit the html files listed in the table in Step 3.

   To include an image in the emails, host the image on a website or save the image in the Portal Website\assets\images folder (C:\inetpub\Portal Website\assets\images, by default), and include a link in the html file.

   Note: If Portal is hosted on a web farm and you save the logo image file locally, you must save the image file on every UI node in the farm.

6. Copy all files that you edited in Steps 4 and 5 into the …\Portal_Service_Connector\bin\EmailTemplates folder (C:\inetpub\Portal Services Website\Portal_Service_Connector\bin\EmailTemplates, by default).

7. Copy all data deletion email files from the …\Portal_Service_Connector\bin\EmailTemplates folder to the following folders:

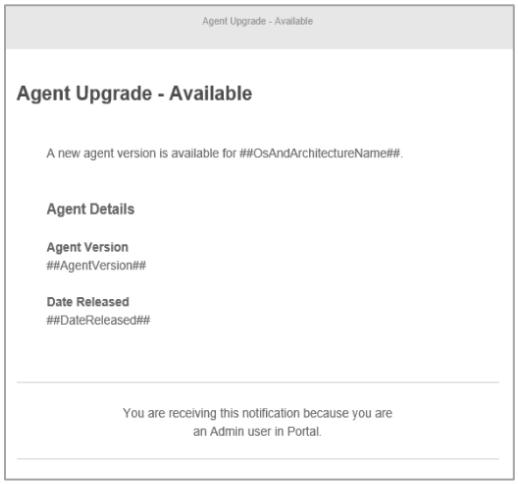
- …\Host_Protect\bin\EmailTemplates (C:\inetpub\Portal Services Website\Host_Protect\bin\EmailTemplates, by default)
- …\Portal Services\API Scheduler\EmailTemplates (by default, C:\Program Files\<*application*>\Portal Services\API Scheduler\EmailTemplates, where <*application*> is “OpenText Server Backup” for fresh Portal installs and “Carbonite Server Backup” for Portal instances that were upgraded from version 9.31 or earlier)

Make sure that you keep backup copies of the edited email files so that they will not be overwritten during future Portal upgrades.

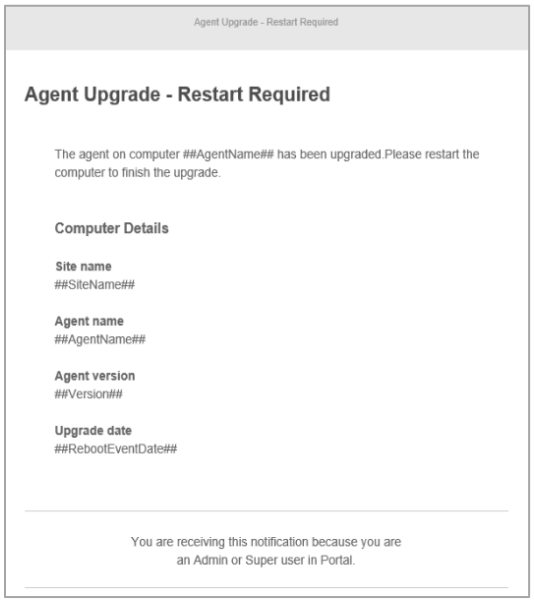
7.1.7 Customize agent auto upgrade emails

You can customize agent auto upgrade emails to include your organization’s text and branding.

If you do not customize agent auto upgrade emails, admin users receive the following unbranded email when a new Windows agent installer is available in their site. The subject line of the email is “Agent Upgrade - Available”.



If you do not customize agent auto upgrade emails, admin users and super users receive the following unbranded email when an upgraded computer needs to be restarted. The subject line of the email is “Agent Upgrade – Restart Required”.


Agent Upgrade - Restart Required

Agent Upgrade - Restart Required

The agent on computer ##AgentName## has been upgraded.Please restart the computer to finish the upgrade.

Computer Details

Site name
##SiteName##

Agent name
##AgentName##

Agent version
##Version##

Upgrade date
##RebootEventDate##

You are receiving this notification because you are an Admin or Super user in Portal.

To customize agent auto upgrade emails:

1. To change the Support phone number, open the web.config file for the Host Protect Service (C:\inetpub\Portal Services Website\Host_Protect\web.config, by default) in a text editor.

   Find the following line:

   ```
   <add key="SupportTelephoneNumber" value="1-866-855-9555" />
   ```

   Replace 1-866-855-9555 with the Support number that you want to include in automatic emails. The resulting line will be something like:

   ```
   <add key="SupportTelephoneNumber" value="1-866-555-0101" />
   ```

2. Find the BrandedTemplates.zip file in the …\Host_Protect\bin\EmailTemplates folder (C:\inetpub\Portal Services Website\Host_Protect\bin\EmailTemplates, by default).

   The BrandedTemplates.zip file contains many email templates and subject lines, including unbranded agent auto upgrade email templates and subject lines.

3. Extract the following files from the BrandedTemplates.zip file:

   - AgentAutoUpgradeAvailable.html
   - AgentAutoUpgradeAvailableSubject.txt
   - AgentAutoUpgradePendingReboot.html
   - AgentAutoUpgradePendingRebootSubject.txt

4. To change the text or appearance of the Agent Upgrade Available email, edit the AgentAutoUpgradeAvailable.html file.
5. To include an image in the email, host the image on a website or save the image file in Portal Website\assets\images (C:\inetpub\Portal Website\assets\images, by default), and include a link in the html file.

   Note: If Portal is hosted on a web farm and you save the logo image file locally, you must save the image file on every UI node in the farm.
6. To change the subject line of the Agent Upgrade Available email, edit the AgentAutoUpgradeAvailableSubject.txt file.

   If you do not edit the .txt file, the email subject line is “Agent Upgrade - Available”.
7. To change the text or appearance of the Agent Upgrade Restart Required email, edit the AgentAutoUpgradePendingReboot.html file.

   To include an image in the email, host the image on a website or save the image in Portal Website\assets\images (C:\inetpub\Portal Website\assets images, by default), and include a link in the html file.
8. To change the subject line of the email, edit the AgentAutoUpgradePendingRebootSubject.txt file.

   If you do not edit the .txt file, the email subject line is “Agent Upgrade – Restart Required”.
9. Save the edited .html and .txt files in the …\Portal Services\API Scheduler\EmailTemplates folder. By default, this folder is C:\Program Files\<*application*>\Portal Services\API Scheduler\EmailTemplates, where <*application*> is “OpenText Server Backup” for fresh Portal installs and “Carbonite Server Backup” for Portal instances that were upgraded from version 9.31 or earlier.

   If you do not save the files in the EmailTemplates folder, users will receive unbranded agent auto upgrade emails.

8 Configure Portal

Note: Before and after Portal configuration changes, we recommend backing up Portal systems as described in Portal Disaster Recovery.

8.1 Configure Portal SSL use

Beginning in version 8.85, Portal uses Secure Sockets Layer (SSL) by default. For Portal to use SSL, choose the https protocol when installing Portal and apply a signed certificate after Portal is installed. Make sure that the certificate matches the domain name that you are using for Portal, and import the certificate into IIS after the Portal installation is complete.

Note: If a load balancer will handle https connections to the Portal UI, the certificate is on the firewall/load balancer and Portal is installed using the http protocol.

If a load balancer will handle connections to the Portal UI, you must change the configuration to not use SSL. You can configure Portal to not use SSL when there is no load balancer, but it is not recommended. See Configure Portal to not use SSL.

If you upgrade Portal to version 8.85 or later, the Portal's SSL settings are carried over from the previous installation. If Portal was previously configured not to use SSL, it will not use SSL after the upgrade. However, you can configure Portal to use SSL. See Configure Portal to use SSL.

8.1.1 Configure Portal to not use SSL

Beginning in version 8.85, Portal is configured to use Secure Sockets Layer (SSL) by default.

If a load balancer will handle connections to the Portal UI, you must also change the configuration to not use SSL.

You can configure Portal to not use SSL when there is no load balancer, but it is not recommended.

To configure Portal to not use SSL:

1. In a text editor, open the config file for the Portal Website (C:\inetpub\Portal Website\web.config).
2. Find the following line in the Portal Website web.config file:

   ```
   <httpCookies httpOnlyCookies="true" requireSSL="true" />
   ```

   Change the requireSSL value to "false". The resulting line should be:

   ```
   <httpCookies httpOnlyCookies="true" requireSSL="false" />
   ```
3. Find the following line in the Portal Website web.config file:

   ```
   <forms loginUrl="~/Account/LogOn" name="PortalAuth"
   requireSSL="true" />
   ```

   Change the requireSSL value to “false”. The resulting line should be:

```
<forms loginUrl="~/Account/LogOn" name="PortalAuth"
requireSSL="false" />
```

4. Save the Portal website web.config file.
5. If Portal was installed using the https protocol, do the following:
   a. In a text editor, open the config file for the Host Protect service (C:\inetpub\Portal Services Website\Host_Protect\web.config).
   b. Find the following line in the Host Protect web.config file:

      ```
      <add key="PortalWebsiteProtocol" value="https" />
      ```

      Change the value from "https" to "http". The resulting line should be:

      ```
      <add key="PortalWebsiteProtocol" value="http" />
      ```

   c. Save the Host Protect web.config file.

8.1.2 Configure Portal to use SSL

If you upgrade Portal to version 8.85 or later, the Portal's SSL settings are carried over from the previous installation. Prior to version 8.85, Portal was installed with SSL settings turned off. If you are running Portal in HTTPS mode and had initially installed a Portal version earlier than 8.85, you should manually update your configuration files to enable the SSL settings.

To configure Portal to use SSL:

1. Make sure you have a certificate that matches the domain name that you will be using for Portal, and import the certificate into IIS.
2. In a text editor, open the config file for the Portal Website (C:\inetpub\Portal Website\web.config).
3. Find the following line in the Portal Website web.config file:

   ```
   <httpCookies httpOnlyCookies="true" requireSSL="False" />
   ```

   Change the requireSSL value to "True". The resulting line should be:

   ```
   <httpCookies httpOnlyCookies="true" requireSSL="True" />
   ```

4. Find the following line in the Portal Website web.config file:

   ```
   <forms loginUrl="~/Account/LogOn" name="PortalAuth"
   requireSSL="False" />
   ```

   Change the requireSSL value to “True”. The resulting line should be:

   ```
   <forms loginUrl="~/Account/LogOn" name="PortalAuth"
   requireSSL="True" />
   ```

5. Save the Portal website web.config file.

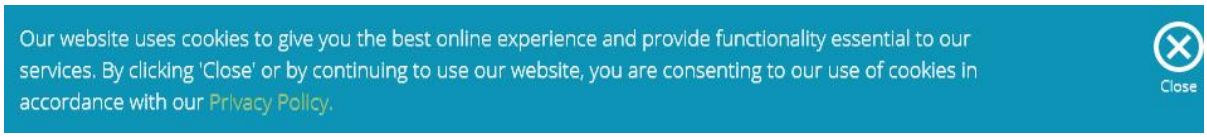
6. In a text editor, open the config file for the Host Protect service (C:\inetpub\Portal Services Website\Host_Protect\web.config).
7. Find the following line in the Host Protect web.config file:

   ```
   <add key="PortalWebsiteProtocol" value="http" />
   ```

   Change the value from "http" to "https". The resulting line should be:
   ```
   <add key="PortalWebsiteProtocol" value="https" />
   ```
8. Save the Host Protect web.config file.

8.2 Specify privacy policy URLs

A message at the bottom of the Portal sign-in page informs users that the Portal website uses cookies. This message, shown below, appears on the sign-in page until a user clicks "Close" in the message box.



The message includes a privacy policy link. By default, the privacy policy URL is https://s3.amazonaws.com/release-notes-information/Privacy+Policy.pdf. You can change the URL to your company's privacy policy, and specify a different URL for each language in the Portal instance.

To specify privacy policy URLs:

1. Open the web.config file for the Portal Website (in C:\inetpub\Portal Website, by default) in a text editor.
2. If the following line appears in the <appSettings> element, delete the line:

   ```
   <add key="PrivacyPolicyUrl" value="yourPrivacyPolicyURL" />
   ```

   Where *yourPrivacyPolicyURL* is the URL for your company's privacy policy (e.g., `https://www.mycompany.com/terms-of-use/privacy-policy/`).
3. In the <configSections> element, add the following line:

   ```
   <section name ="PrivacyPolicy" type
   ="EVault.Web.Integration.PrivacyPolicy.PrivacyPolicyConfigu
   ration, EVault.Web.Integration, Culture=neutral"/>
   ```
4. In the <configuration> element, add the following section:

   ```
   <PrivacyPolicy>
       <PrivacyPolicies>
        <add name = "language" Url ="privacyPolicyURL" />
   ```

```
    </PrivacyPolicies>
</PrivacyPolicy>
```

Where:

- *language* is a language in the Portal instance: en-US (English – United States), en-UK (English – United Kingdom), fr-FR (French), de-DE (German) or es-ES (Spanish)
- *privacyPolicyURL* is a valid, accessible link to the privacy policy in the specified language.

5. In the <PrivacyPolicy> element, add an `<add name… />` line for each language in the Portal instance. The resulting section could be something like:

```
<PrivacyPolicy>
    <PrivacyPolicies>
      <add name = "en-US" Url
="https://www.mycompany.com/terms-of-use/privacy-policy/"
/>
      <add name = "fr-FR" Url
="https://s3.amazonaws.com/release-notes-
information/Privacy+Policy-FR.pdf" />
      <add name = "es-ES" Url
="https://s3.amazonaws.com/release-notes-
information/Privacy+Policy-ES.pdf" />
    </PrivacyPolicies>
</PrivacyPolicy>
```

6. Save the web.config file.

8.3 Configure a web farm

A web farm uses multiple web servers to distribute your UI processing load across servers. If you need more processing power, you can add another server without changing your Portal configuration or installation. The web farm uses a virtual IP address (to which your UI application points) that is then resolved into physical addresses for the servers.

Agents must be registered to the IP address of the AMP Redirector service.

The Administrator is responsible for installing and configuring the web farm. This includes setting the IP addresses, masks and gateways, and network load balancing. These functions are not covered in this guide.

You can install back-end Portal components on one server (which is not part of the farm). You can then install the Portal UI on each server in the web farm.

There can be multiple AMP Proxy servers, each of which can support up to 1800 registered agents. Each AMP Proxy should be installed on its own system (not the UI system). Beginning in Portal 9.10, you can also install multiple Redirectors behind a load balancer.

All components on a web farm must be the same version. If you are upgrading, you must upgrade all components on all servers to the same version.

Notes:

- The UI Web application can support up to 50 concurrent user connections per server. If you need more, you must use a web farm for multiple servers.
- The Load Balancer must be configured to use sticky sessions.
- The Task Scheduler and API Scheduler should only run on one Portal UI server in a web farm.

In Portal versions earlier than 8.88, you had to enter machine keys in Portal configuration files when setting up a web farm. Beginning in Portal 8.88, machine keys are populated in Portal configuration files when you install or upgrade Portal components.

To configure a web farm:

1. Install the Notification Service, Registration Service and SQL Server on one machine (not a part of the farm) as described in Install back-end system components. This server does not expose anything to the internet so does not need to be accessible by agents.
2. Install the Proxy and Redirector on one or more servers which are externally accessible. Run the installation on each machine as described in Install AMP Proxies and Redirectors. Agents will need to connect to these servers over ports 8086 and 8087.

   If you have more than 1800 agents connecting to this environment, you will need to install more than one Proxy. Beginning in Portal 9.10, you can also install multiple Redirectors behind a load balancer. See Install AMP Proxies and Redirectors and Configure load balancing for multiple Redirectors.
3. Install the Portal UI on each of the farm servers as described in Install front-end system components.
4. On all Portal UI servers except one, shut down the following services:
   - OpenText Server Backup Task Scheduler
   - OpenText Server Backup API Scheduler

   The Task Scheduler and API Scheduler should only run on one Portal UI server in a web farm.

8.4 Configure load balancing for multiple Redirectors

Beginning in Portal 9.10, you can install multiple AMP Redirectors in a distributed Portal instance.

An HTTP endpoint is exposed for checking the health of a Redirector service. See HTTP health check endpoint for the Redirector service. You must configure the health check endpoint for each Redirector. See Configure the Redirector Health Check Endpoint.

You can then configure a load balancer (e.g., F5) to check the health of each Redirector service and only route requests to healthy services. See Example: Configure a load balancer for Portal Redirectors.

8.4.1 Health check endpoint for AMP Redirector

Beginning in Portal 9.10, an HTTP endpoint is exposed for checking the health of an AMP Redirector. To check the health of a local AMP Redirector service, you can:

- Use an HTTP request to access the health check endpoint:

  ```
  http://localhost/redirector/api/health/hc
  ```

  If the service is functional, the endpoint returns:

  ```
  <ArrayOfHealthStatusNode>
  <HealthStatusNode>
  <LastStatusUpdateTimestamp>2022-06-21T10:51:18.522755-
  04:00</LastStatusUpdateTimestamp>
  <ServiceHealthTask>RedirectorStatus</ServiceHealthTask>
  <Status>Healthy</Status>
  </HealthStatusNode>
  </ArrayOfHealthStatusNode>
  ```

- Run a PowerShell command to access the health check endpoint:

  ```
  iwr -useb http://localhost/redirector/api/health/hc
  ```

  If the service is functional, the endpoint returns:

  ```
  StatusCode        : 200
  StatusDescription : OK
  Content           :
  [{"Status":"Healthy","LastStatusUpdateTimestamp":"2022-06-
  21T16:16:02.9198393-
  04:00","ServiceHealthTask":"RedirectorStatus"}]
  ```

8.4.2 Configure the Redirector Health Check Endpoint

Before configuring a load balancer, you must configure the Redirector nodes to ensure that they will respond to health check endpoint queries.

Configure the Health Check Endpoint URL

Do the following on each server where the Redirector is installed:

1. In a text editor, open the RedirectorService.exe.config file (by default, in C:\Program Files\<*application*>\Portal Services\AMP Redirector Service, where <*application*> is "OpenText Server Backup" for fresh Portal installs and "Carbonite Server Backup" for Portal instances that were upgraded from version 9.31 or earlier).
2. Find the following line:
   ```
   <add key="Redirector.HealthAPI.Url"
   value="http://localhost/redirector" />
   ```
3. Replace `localhost` with the IP address or hostname of the server where the Redirector is running. For example, the resulting line could be:

```
<add key="Redirector.HealthAPI.Url"
value="http://192.0.2.1/redirector" />
```

or

```
<add key="Redirector.HealthAPI.Url"
value="http://redirector.portal.local/redirector" />
```

Note: Do not remove "redirector" from the end of the line. This forms the basis for the remainder of the health check endpoint (e.g., http://192.0.2.1/redirector/api/health/hc).

4. Save the RedirectorService.exe.config file.
5. Restart the Redirector service.

(If required) Configure the Health Check Endpoint port

By default, the Redirector health check endpoint is listening on port 80, like any normal web service.

If other web services are installed on the system where the Redirector is installed, you must either:

- Install IIS (recommended). IIS can automatically manage web services on port 80. You can install IIS from Windows PowerShell (with administrative privileges) using the command install-windowsfeature web-server. It requires no configuration if you are installing it to support routing multiple health check endpoints, and no other IIS components are required.

- Specify a different port for the health check endpoint. To do this, edit the RedirectorService.exe.config file (by default, in C:\Program Files\Carbonite Server Backup\Portal Services\AMP Redirector Service, where *<application>* is "OpenText Server Backup" for fresh Portal installs and "Carbonite Server Backup" for Portal instances that were upgraded from version 9.31 or earlier) as described in Configure the Health Check Endpoint URL and add the port number after the redirector URL. For example, to make the health check available on port 8080, the line would be:

```
<add key="Redirector.HealthAPI.Url"
value="http://192.0.2.1:8080/redirector" />
```

Note: You will need to open this port on the Windows firewall if it is not already open. You can do this by running the following command from a PowerShell window with administrative privileges:

```
New-NetFirewallRule -DisplayName "TCP Port 8080 for Redirector
Health Check" -Direction inbound -Profile Any -Action Allow -
LocalPort 8080 -Protocol TCP
```

8.4.3 Example: Configure a load balancer for AMP Redirectors

Using the health check endpoint for AMP Redirector services, you can configure a load balancer that checks the health of each Redirector and only sends requests to Redirectors that are available.

This section provides an example of how to configure a load balancer for AMP Redirectors using the following steps:

1. Create a health monitor
2. Create parent nodes
3. Create a pool and add nodes
4. Configure a virtual server
5. Test the load balancer

This example is based on older F5 Big-IP firmware (dated 2012). Administrative rights were required on the F5 to perform the required operations.

Steps for configuring load balancing will vary, depending on your load balancer and environment.

8.4.3.1 Create a health monitor

The first step in this example is creating a health monitor. The health monitor is responsible for determining whether Registration services are available and capable of receiving incoming requests.

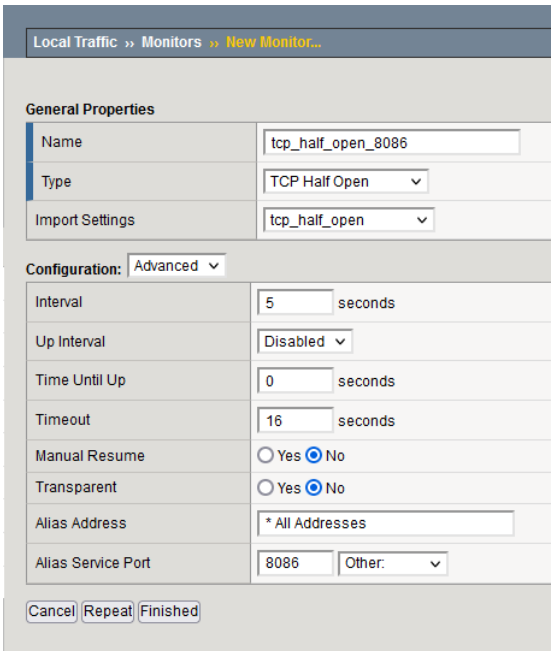
This example shows how to create either a:

- TCP health monitor. Many options are available for creating health monitors. In this example, we create a TCP Half Open health monitor. TCP Half Open does not try to complete a TCP connection, which reduces the chance that your logs will fill up with broken connection error messages.
- HTTP health monitor. F5 Big-IP does not have native functionality for consuming JSON or XML health check data. Instead, it performs regex operations on raw text returned from HTTP requests (GET, POST, etc) to a given URL. For more information, see the F5 documentation.

To create a health monitor:

1. In the F5 interface, on the left side under Local Traffic, click **Monitors**, and then click the **Create** button in the upper right. You can also click the green plus sign in the menu.
2. On the General Properties screen, do one of the following:
3. Do one of the following:
    - To create a TCP health monitor, select **TCP Half Open** as the Type. The screen then reloads and shows more options.

      The following screen shows TCP Health Monitor properties for port 8086, the Redirector's service port. It uses the default *Interval* of 5 seconds and the default *Timeout* of 16 seconds. The longer these values are, the more likely it is that the service will fail to connect a request to a working node if one of the nodes fails.



- To create an HTTP health monitor, select **HTTP** as the Type.

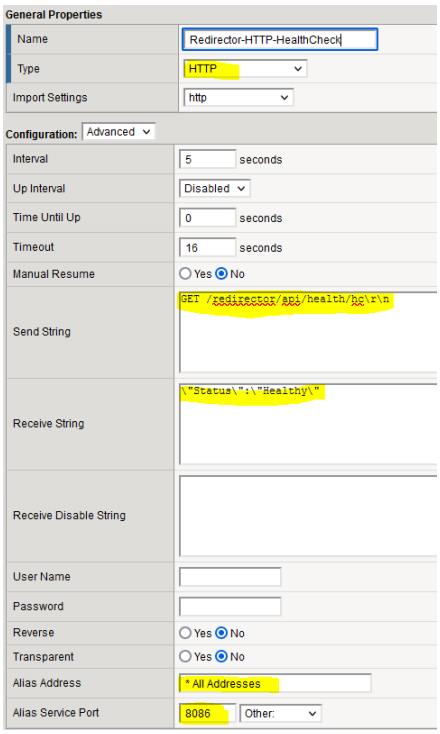
  The following screen shows HTTP health monitor properties. The most important entries are the *Send String*, *Receive String and Service Port.*

  The *Send String* is an HTTP request that returns the following JSON health check payload:

```
"RedirectorStatus": {
    "Status": "Healthy",
    "LastStatusUpdateTimestamp": "2022-06-02T13:04:55.4973741-
04:00",
    "ServiceHealthTask": "RedirectorStatus"
}
```

  The *Receive String* is a regex expression that looks for the following string in the JSON payload: "Status": "Healthy". The backslashes are necessary to escape the quotes as quotes are operators in regex.

  The *Service Port* is the port specified for the health check endpoint in the RedirectorService.exe.config file (by default, in C:\Program Files\<*application*>\Portal Services\AMP Redirector Service, where <*application*> is “OpenText Server Backup” for fresh Portal installs and “Carbonite Server Backup” for Portal instances that were upgraded from version 9.31 or earlier). By default, the health check endpoint is 80 but you might have changed it as described in Configure the Health Check Endpoint port.



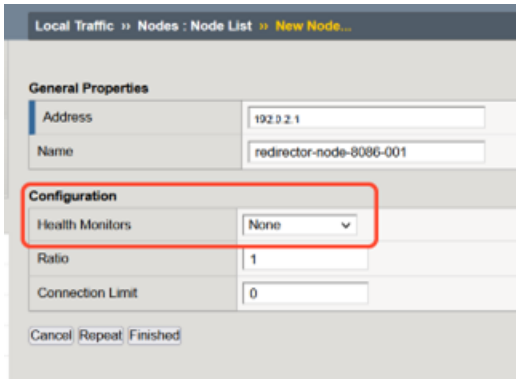
4. When you are finished, click the **Finished** button.

8.4.3.2 Create Redirector nodes

Before creating a pool of AMP Redirector nodes for load balancing, you must create the nodes. These are the individual Redirector addresses that the F5 will send traffic to when it routes connections.

To create Redirector nodes:

1. In the F5 interface, click **Nodes**, click **Node List**, and then click the **Create** button. You can also click the green plus sign next to Node List in the menu.
2. Configure as shown in the following screen. In the Health Monitors list, choose "None". This allows the nodes to inherit their Health Monitor behavior from the pool.



3. Click **Repeat** to create another node. Click **Finished** if you are done.

8.4.3.3 Create a pool and add nodes to the pool

To create a pool and add nodes to the pool:

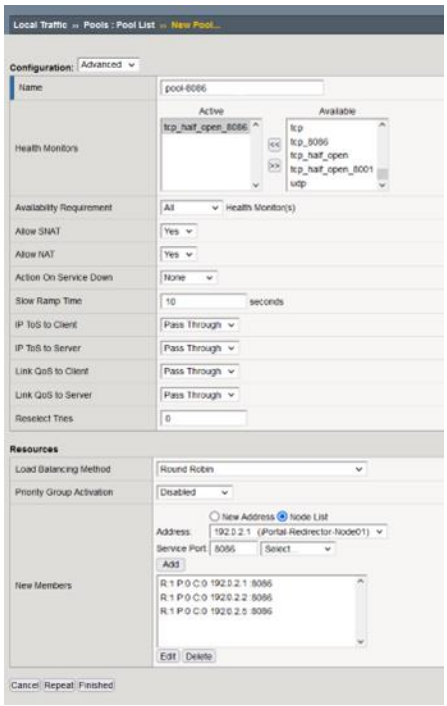
1. In the F5 interface, click **Pools**, click **Pool List**, and then click the **Create** button. You can also click the green plus sign next to Pool List in the menu.
2. Configure the pool as shown in the following screenshot. The settings shown are for a pool of three Redirector nodes. operating on port 8086.

   Add the health monitor created in Create a health monitor.

   Make sure that **Allow Snat** is set to **Yes**.

   Choose a load balancing method (e.g., Round Robin).

   Select the **Node List** radio button. Add each of the Redirector nodes that you created in Create Redirector nodes.



3. Click **Finished** when done.

8.4.3.4 Configure a virtual server

Finally, you can configure a virtual server. The virtual server receives incoming traffic and distributes it to the nodes.

To configure a virtual server:

1. In the F5 interface, click **Local Traffic**, click **Virtual Servers - Virtual Server List** and then click **Create**. You can also click the green plus sign in the menu.

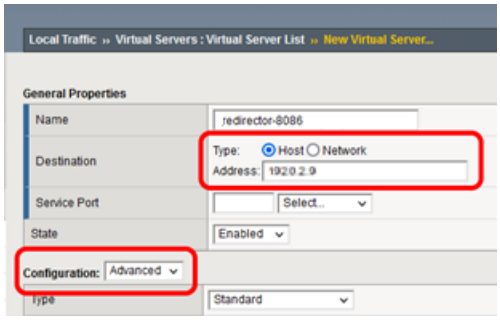
2. Configure the server as shown in the following screenshot. The settings shown are for a virtual server that services a pool of AMP Redirector nodes on port 8086.

   In the **Name** field, enter a unique, descriptive name, preferably one that includes the service name and port number.

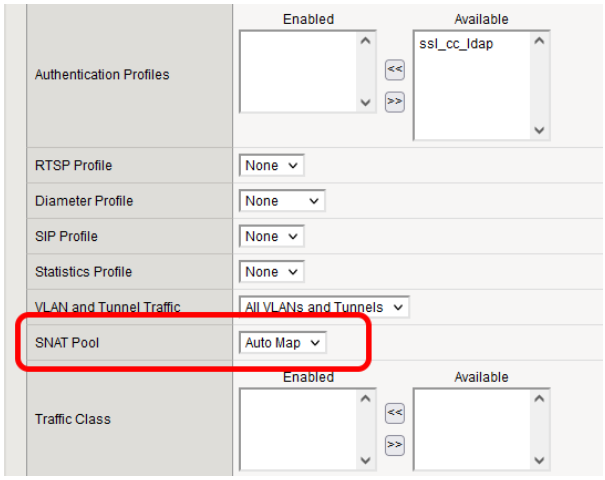
   In the **Destination: Address** field, enter the IP address. The **Type** should be set to **Host**

   In the **Service Port** field, enter **8086.** Entering this value sets the dropdown menu to Other.

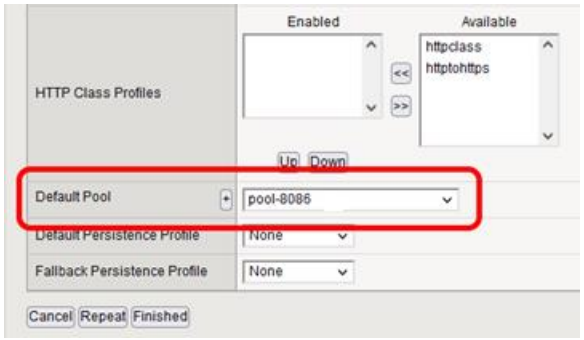
   Make sure **Configuration** is set to Advanced.



   Change **SNAT Pool** to **Auto Map**.



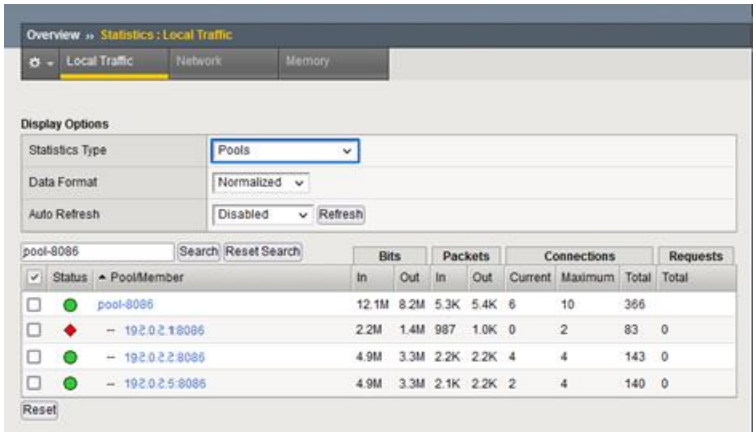
   Set the **Default Pool** to the pool you created in Create a pool and add nodes to the pool.



3. Click **Finished** when done.

8.4.3.5 Test the load balancer

At this point, the load balancer should be ready to use. You can test your service and make sure that packets are going where they are supposed to by checking the statistics of the various components. The most useful are probably the pool node statistics, which you can find by clicking on the pool, and then the **Statistics** link:



Here, we see that one node has been down for a while, so the amount of traffic distributed to the other two nodes is much higher. We can see information such as how many connection attempts have been made, the amount of data in and out, and the packets in and out.

Every object has its own statistics like this. You can use this information to determine how your nodes are behaving and whether your load balancing method (e.g., Round Robin) is working as expected.

8.5 Configure load balancing for multiple Notification services

Beginning in Portal 9.20, you can install multiple Notification services in a distributed Portal environment. You can then configure a load balancer (e.g., F5) to route requests to available Notification services and enter load balancer information in Notification service config files, as described in the following example.

8.5.1 Example: Configure a load balancer for Notification services

This section provides an example of how to configure a load balancer for Notification services using the following steps:

1. Create a health monitor
2. Set up X-Forwarded-For HTTP Header
3. Create Nodes
4. Create Pool

5. Create a Virtual Server for the Notification Service
6. Verify Proxy and F5 communication
7. Specify Load Balancer information in Notification Service config files
8. Test the Notification Service Functionality through the Load Balancer

This example is based on older F5 Big-IP firmware (dated 2012). Administrative rights were required on the F5 to perform the required operations.

Steps for configuring load balancing will vary, depending on your load balancer and environment.

8.5.1.1 Create a health monitor

First, we need to set up a health monitor on F5 which can utilized by the Notification service pool to mark the nodes as online or offline. The Notification service health monitor setup is similar to the health monitor setup for the Redirector.

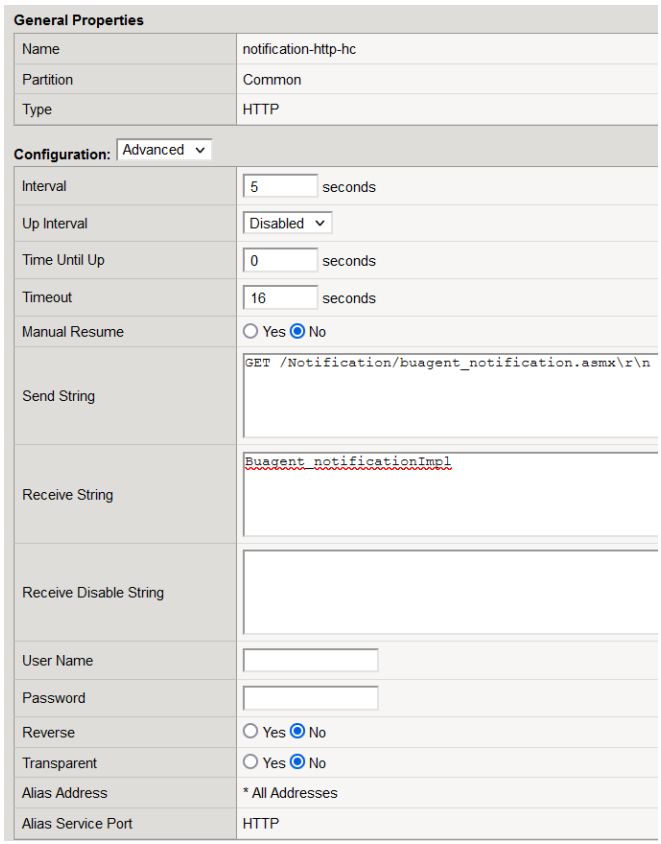
1. Log in to the F5 UI.
2. On the left pane menu, expand Local Traffic and select Monitors.
3. Click the Create button to configure a new health monitor.
4. Provide a name for this monitor and select the "HTTP" type.
5. Under Advanced Configuration, set the Send String to:

   ```
   GET /Notification/buagent_notification.asmx\r\n
   ```

6. Set the Receive String to:

   ```
   Buagent_notificationImpl
   ```

7. Set Alias Service Port as HTTP (Port 80).
8. The rest of the configuration can be left with default values. Click **Finish** to save the configuration.



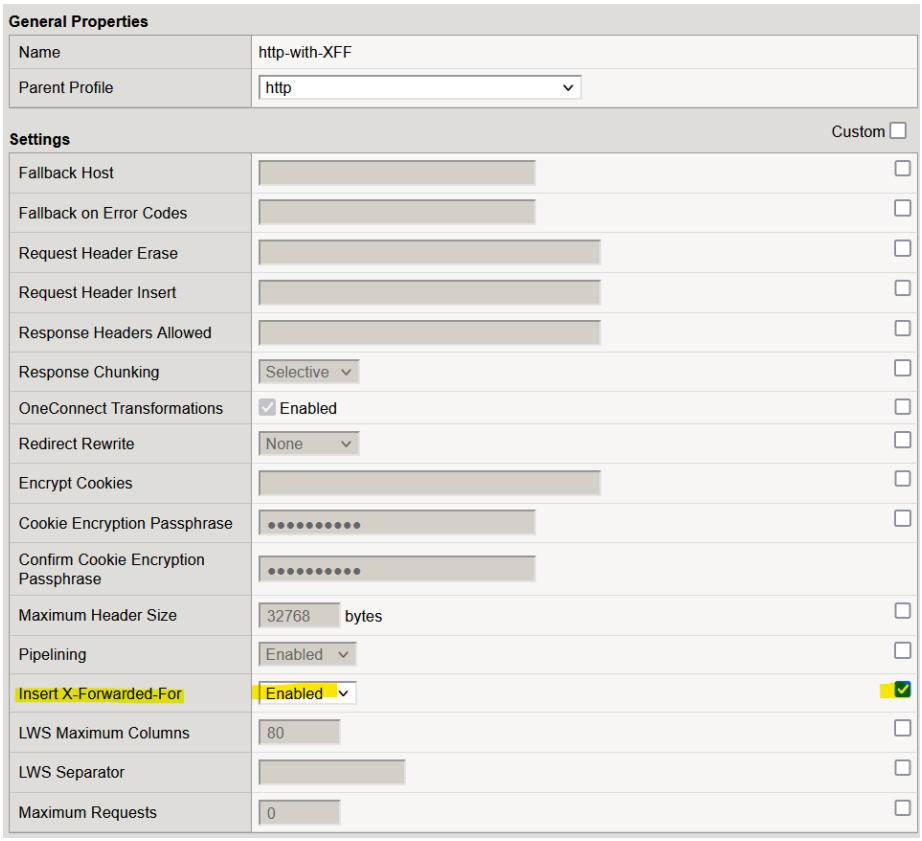
General Properties	
Name	notification-http-hc
Partition	Common
Type	HTTP
Configuration: Advanced	
Interval	5 seconds
Up Interval	Disabled
Time Until Up	0 seconds
Timeout	16 seconds
Manual Resume	Yes / No
Send String	GET /Notification/buagent_notification.asmx\r\n
Receive String	Buagent_notificationImpl
Receive Disable String	
User Name	
Password	
Reverse	Yes / No
Transparent	Yes / No
Alias Address	* All Addresses
Alias Service Port	HTTP

8.5.1.2 Set up X-Forwarded-For HTTP Header

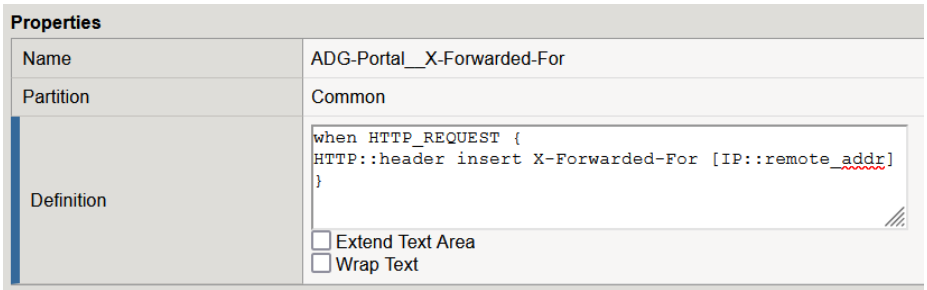
Next, we need to create a profile and iRule to insert the X-Forwarded-For header in the requests being forwarded to the Notification service. This will ensure that we are sending the Proxy IP address to the Notification service which it will use to validate that the request is coming from an authorized Proxy server. If this header is not configured then the Notification service will report failures for this missing header - *"A load balancer has been defined, but the HTTP_X_FORWARDED_FOR header is not present. This header must be specified for security reasons."*

To configure the profile and iRule to insert the X-Forwarded-For header, see the F5 documentation. The final configuration should look like this:

- Profile:



- iRule:

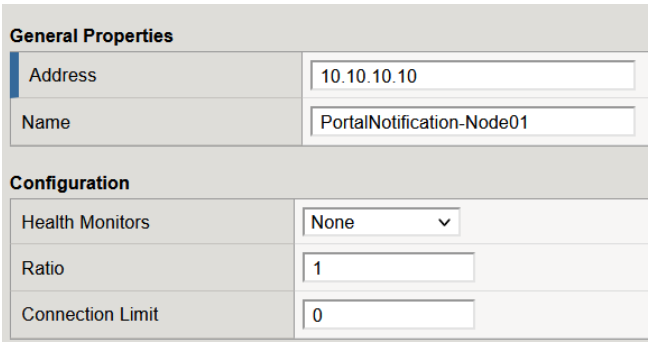


8.5.1.3 Create Nodes

Create a node for each instance of the Notification service which can be added to the pool in the next steps.

1. On the left pane menu, expand Local Traffic and select Nodes.
2. Click Create button to add a node.

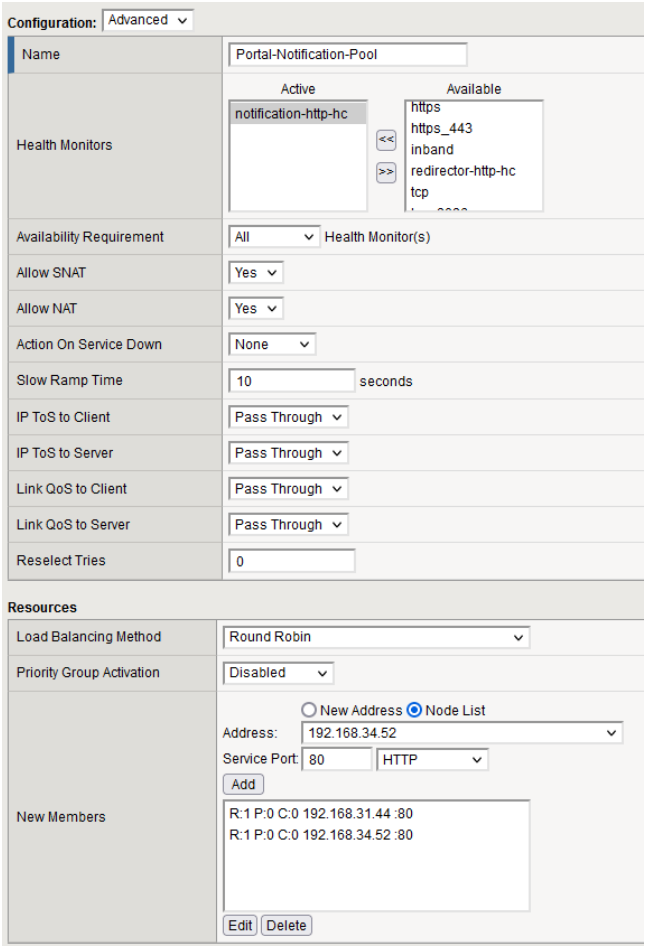
3. Specify the IP address or FQDN of the server where Notification service is installed.
4. Provide a name for this node.
5. Set Health Monitors to "None" and click Finished.
6. Repeat steps 1-5 to add all of the Notification service nodes.



8.5.1.4 Create Pool

Create a pool to use for load balancing the Notification service. The pool includes all Notification service nodes.

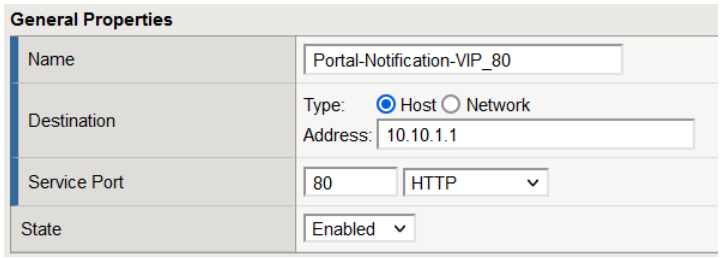
1. On the left pane menu, expand Local Traffic and select Pools.
2. Click Create button to add a pool. Make sure Configuration mode is set to Advanced.
3. Specify a name for this pool.
4. In the Health Monitors field, add the monitor created for Notification service. This monitor will be applied to all the nodes under the pool.
5. Specify the Load Balancing Method as "Round Robin".
6. For New Members field, select the radio button for "Node List" and select the Service Port as "HTTP". Click Add and repeat for each node.
7. Click Finished and save the configuration.



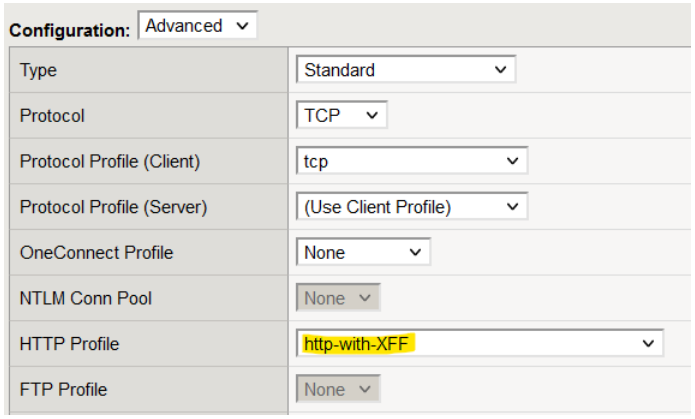
8.5.1.5 Create a Virtual Server for the Notification Service

Before creating a virtual server in F5, we need to get an IP address that can be exclusively used for setting up the virtual server. This IP will be used by the Proxy to make BANS calls which will then be forwarded to actual Notification service nodes by the F5.

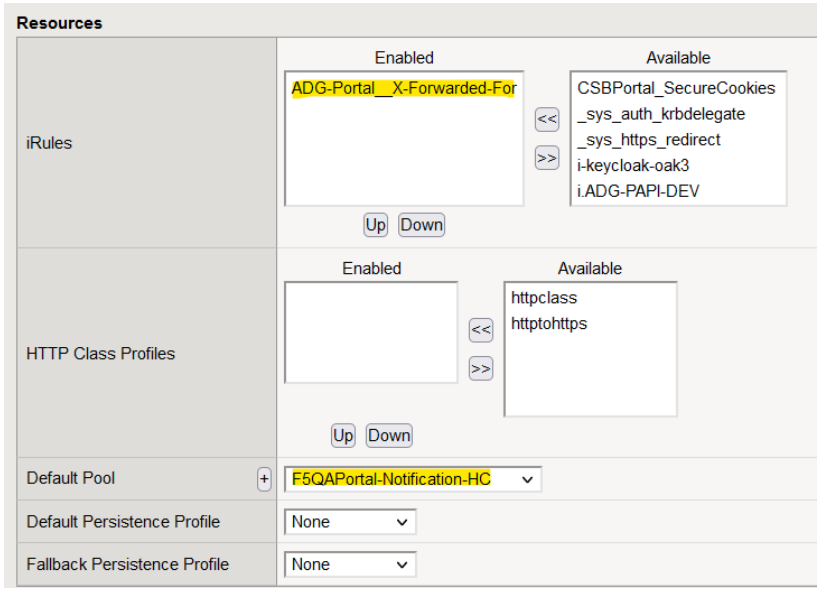
1. Login to the F5 UI.
2. On the left pane menu, expand Local Traffic and select Virtual Servers.
3. Click Create button to configure a new virtual server for the Notification service.
4. Under General Properties, provide a name for this virtual server.
5. Specify the Destination IP address.
6. Set the Service Port to HTTP (Port 80).



7. Switch to Advanced configuration.
8. Select HTTP Profile as the one created for Notification service in step 2.



9. In the iRules section, enable the iRule for X-Forwarded-For header created in step 2.
10. Select the Default Pool as the one defined in step 4 for Notification service. Click Finished to create the virtual server.



8.5.1.6 Verify Proxy and F5 communication

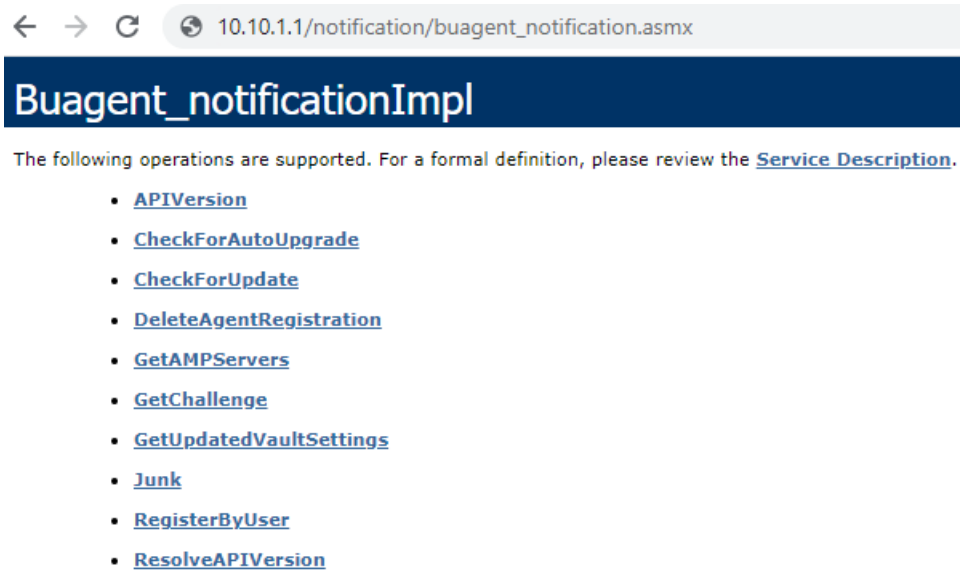
After the F5 setup is complete, we must verify access to the Notification service virtual IP address from each of the AMP Proxy servers. Do the following on each Proxy server:

1. Login to Proxy server and run this PowerShell command to ensure access on port 80:

   ```
   tnc 10.10.1.1 -port 80
   ```

   Replace the IP with the IP address of your virtual server.

2. In a web browser, verify access to Notification service endpoint by browsing to http://*10.10.1.1*/Notification/buagent_notification.asmx. Replace the IP address with the IP address of your virtual server.



Next, we need to update the Proxy config file to use the load balancer IP for Notification service. On each Proxy server:

3. Open File Explorer and go to C:\Program Files\<*application*>\Portal Services\AMP Proxy Service, where <*application*> is “OpenText Server Backup” for fresh Portal installs and “Carbonite Server Backup” for Portal instances that were upgraded from version 9.31 or earlier.

4. Open the AmpService.exe.config file in a text editor like Notepad.

5. Search for the following line:

   ```
   <add key="WebService.Notification.Url"
   value="http://192.168.1.1/Notification/buagent_notification
   .asmx" />
   ```

   Replace the IP with the load balancer virtual server IP from step 5. Save the changes and restart AMPProxy service.

6. If the virtual server IP is 10.10.1.1, then the modified value in Proxy config file will be:

   ```
   <add key="WebService.Notification.Url"
   value="http://10.10.1.1/Notification/buagent_notification.asmx" />
   ```

8.5.1.7 Specify Load Balancer information in Notification Service config files

Finally, the Notification service config file needs to specify the use of load balancer to make sure the calls are being forwarded from the F5 to the Notification server(s).

Do the following on each server where Notification service is installed:

1. Open File Explorer and go to C:\inetpub\Portal Services Website\Notification.
2. Open Web.config file in a text editor like Notepad.
3. Add the following line in the <appSettings> section:

   <add key="LoadBalancer.OutgoingOrigin.Address" value="*192.10.2.1*" />

   Replace the IP with the IP address used by your F5 setup to forward the requests to the Notification service. This IP need not be the virtual server IP defined in step 5, instead this can be one of the Self-IPs configured on F5 under the Network section. For more information, see the F5 documentation.

8.5.1.8 Test the Notification Service Functionality through the Load Balancer

Confirm that the service is in a functional state by making some BANS call to the Notification service. A BANS call can easily be triggered by running a backup job using the Portal UI. If everything is in order, the Notification service on all nodes should not report any errors.

The calls made by the Proxy service should finish successfully and report no errors in the log file.

9 Modify Portal

You can change which Portal components are installed on a server by running the Portal installation kit. You can also change the languages that are installed.

If Portal was installed on a single system, and you want to change it to a distributed system, see Convert Portal from a single system to a distributed system.

The installers automatically shut down services on the machine where you are modifying components. However, if Portal is installed on a distributed system, shut down services on other machines before modifying your installation.

Note: Before modifying Portal and after any configuration changes, we recommend backing up Portal systems as described in Portal Disaster Recovery.

To modify Portal:

1. On the machine where you want to modify components, run the Portal installation kit.
2. On the Welcome page, click **Modify**, and then click **Next**.
3. On the SQL Server Setup page, choose the SQL Server instance where the databases will be installed. Specify the authentication method, and then click **Next**.

   You can optionally click **Test** to validate the connection with the database server.

   The Select Features page appears. Components that are currently installed on the server are selected on this page.
4. Select the check box for each component that you want to add or keep. Clear the check box for each component that you want to uninstall.
5. Click **Next**.
6. On the remaining installation wizard pages, provide the required information.

   Wizard pages that appear depend on the components selected on the Select Features page. For information about specific pages, see Install Portal on a single system.
7. In the confirmation dialog box, click **OK**.

   After the components are installed, a Component Status page appears. This page indicates which components have been installed and which components need to be installed before the system will be operational.

   The page also indicates if one of the components is not at the same versions as the other components and will still need to be upgraded. Components which are currently installed, but are not up to the current version, may show as missing.
8. Click **Next**.
9. Click **Finish**.

9.1 Convert Portal from a single system to a two-server distributed system

To convert Portal from a single system to a distributed system, you can move front-end components to a new server. Moving back-end Portal components to a new server is not recommended, as this process would require database migration and is more complex than moving front-end components.

In the two-server distributed system created using this procedure, the Portal UI is installed on the same system as the Redirector and Proxy. Although this configuration differs from the large-scale distributed system shown in Portal – Distributed System (recommended), it can support more Agents than when all Portal components are installed on a single system (recommended for fewer than 500 Agents). A two-server distributed system can also serve as an interim step in moving to the recommended distributed system. You can later add a load balancer and multiple Portal UI machines, or multiple proxies. See Configure a web farm.

Note: Beginning in Portal 8.88, when you convert Portal from a single system to a two-server distributed system, you must create a text file that contains a machine key for Portal configuration files. This file is required when you install front-end components on a new server.

This procedure is applicable to Portal version 8.88 or later. For an earlier Portal version, see the *Portal Installation and Configuration Guide* for that version.

Note: Before modifying Portal and after any configuration changes, we recommend backing up Portal systems as described in Portal Disaster Recovery.

To convert Portal from a single system to a two-server distributed system:

1. Prepare a new server for installing Portal front-end components. For system requirements, see Prerequisites and recommendations and the Portal release notes.
2. On the server where Portal is installed, check that Portal version 8.88 or later is installed.
3. Do the following to create a text file that contains the machine key for the Portal instance:
    a. On the server where Portal is installed, in a text editor, open the Web.config file for the Portal UI (C:\inetpub\Portal Website\Web.config).
    b. In the Web.config file, look for a line that starts with "<machineKey ". The machineKey line should be in a <system.web> element and be something like:

```
<machineKey decryption="AES"
decryptionKey="6406C768ED214DD93F0EC68D5E18D0DA6FE4ABE44C588149
"
validationKey="E360EA1C515E2B9216AF500DF8EA2AA28C9418EA2F1B978B
CC6185E5075219B656A1E1EC6B2986DB9A8AC8B6BD370F547BC1A644C77B313
F8B35E456D8C37739" />
```

c. Copy the entire machineKey line from the Web.config file for the Portal UI.

d. In a text editor, create a new text file. In the new text file, paste the machineKey line from the Web.config file for the Portal UI.

e. Save the new text file with the .txt file extension (e.g., PortalKey.txt). Be sure to keep a backup copy of this file somewhere safe.

4. On the server where Portal is installed, run the Portal installation kit. When the Welcome page appears, do the following to populate a required value in the database:

a. In the %temp% directory on the server, look for a subdirectory that was created at the same time that you ran the installation kit, is named with a series of letters and numbers (e.g., {04FA0F97-4596-4BD6-9F2E-48439AD54AEA}), and contains files named MachineKeyTester.exe and MachineKeyTester.exe.config.

b. Copy the entire subdirectory found in Step a. Paste the subdirectory in another location on the server.

c. In a text editor, open the MachineKeyTester.exe.config file from the subdirectory that you pasted in Step b.

d. In the MachineKeyTester.exe.config file, do the following:

- Find the line that starts with `<add name="SiteManagement.Sql.Connection"`. Replace the line with the line in the web.config file for the Notification Service (in C:\inetpub\Portal Services Website\Notification\web.config). The line should be in an appSettings element and be something like:

```
<add key="SiteManagement.Sql.Connection" value="Data
Source='PORTAL';Initial
Catalog='SiteManagement';Integrated Security=SSPI" />
```

- Find the line that starts with "`<machineKey `". Replace the machineKey line with the machineKey line from the text file created in Step 3.

e. Save the MachineKeyTester.exe.config file.

f. At a command prompt, navigate to the subdirectory where the edited MachineKeyTester.exe.config file is located, and run the following command:

```
MachineKeyTester.exe save Portal
```

5. On the server where Portal is installed, click **Next** on the Welcome page to continue running the Portal installation kit. Uninstall the following front-end components:

- AMP Redirector Service
- AMP Proxy

- Portal UI

For more information, see Modify Portal.

6. After the uninstallation is complete, open the Internet Information Services (IIS) Manager on the server where you uninstalled Portal front-end components.
7. Right-click “Portal Services Website”, and choose **Edit Bindings**.
8. In the Site Bindings dialog box, click “127.0.0.1”, and then click the **Edit** button.
9. In the Edit Site Binding dialog box, delete “127.0.01” from the **Host name** box. Do one of the following:
   - In the **IP address** list, select an IP address that the new front-end server (prepared in Step 1) can access.
   - In the **Host name** box, enter either the system’s name or its fully qualified domain name (FQDN).

   Note: The Port value in the Edit Site Binding dialog box remains as “80”.
10. Click **OK** to close the Edit Site Binding dialog box.
11. Click **Close** to close the Site Bindings dialog box.
12. Restart the Portal Services Website.
13. On the new server for installing Portal front-end components (prepared in Step 1), log in as an administrator. Copy the Portal installation kit to the server. Copy the machine key text file created in Step 3 to the server.
14. Run the Portal installation kit to install the following front-end components:
    - AMP Redirector Service
    - AMP Proxy
    - Portal UI

    During the installation, on the SQL Server Setup page, specify the SQL Server instance where the Portal databases are installed on the original server.

    On the AMP Service Configuration page, enter the IP address or hostname specified in Step 9 as the Notification service web address.

    On the AMP Redirector Service Configuration page, enter the IP address or hostname specified in Step 9 as the Registration service web address.

    For more information, see Install front-end system components and Install the Proxy and Redirector.

9.2 Install additional Redirectors

Beginning in Portal 9.10, you can install multiple Redirectors in a distributed Portal environment.

If you would like to install an additional Redirector but your Portal components are installed on a single system, you must first convert Portal to a distributed system. See Convert Portal from a single system to a two-server distributed system.

IMPORTANT: When you add an additional Redirector, the Redirector will not be used until the load balancer in the environment is configured as described in Configure load balancing for multiple Redirectors.

To install an additional Redirector:

1. On the server where you want to install an additional Redirector, log in as an administrator.
2. Copy the Portal installation kit to the server. Copy the PortalKey.txt file for the Portal instance to the same location on the server as the installation kit.

   The PortalKey.txt contains a machine key for the Portal instance. This file is created during the database installation or upgrade in a distributed environment, and should be available on the server where Portal back-end components are installed.
3. Run the Portal installation kit.
4. On the Welcome page, click **Next**.
5. On the View Notes page, click **Next**.
6. On the License Agreement page, read the license agreement. Select **I accept the terms of the license agreement**, and then click **Next**.
7. On the SQL Server Setup page, choose the SQL Server instance where the databases are installed. Select **SQL Server authentication**, enter SQL Server credentials, and then click **Next**.
8. On the Select Features page, select **AMP Redirector Service**. Click **Next**.
9. On the AMP Redirector Service Configuration page, enter the Registration Service web address, and then click **Next**.

   We recommend using the internal IP address of the system where the Registration service is installed in the URL. This will avoid any issues with the name resolving to an IPV6 IP address instead of an IPV4 address. For example, if the IP address for the server where the Registration service is installed is 10.51.1.1, use this IP address when installing the second Redirector.

10. On the Redirector Address Configuration page, the IP address of the current server appears. You do not need to change this value. Click **Next**.
11. On the Services/Support Files page, specify the location for installing services and support files, and then click **Next**.
12. On the Machine Key File page, specify the location of the PortalKey.txt file that was copied to the server in Step 2. Click **Next**.
13. In the confirmation dialog box, click **Yes**.

    When finished, a Component Status page shows the version of each installed Portal component.
14. Click **Next**.
15. Click **Finish**.

9.3 Install additional Notification services

Beginning in Portal 9.20, you can install multiple Notification services in a distributed Portal environment.

If you would like to install an additional Notification service but your Portal components are installed on a single system, you must first convert Portal to a distributed system. See Convert Portal from a single system to a two-server distributed system.

IMPORTANT: When you add a Notification service, the Notification service will not be used until the load balancer in the environment is configured and the load balancer IP address is entered in the web.config file for each Notification service. See Configure load balancing for multiple Redirectors.

To install an additional Notification service:

1. On the server where you want to install an additional Notification service, log in as an administrator.
2. Copy the Portal installation kit to the server. Copy the PortalKey.txt file for the Portal instance to the same location on the server as the installation kit.

   The PortalKey.txt contains a machine key for the Portal instance. This file is created during the database installation or upgrade in a distributed environment, and should be available on the server where Portal back-end components are installed.
3. Run the Portal installation kit.

   If a message states that the software is blocked from running, right-click the installation kit and choose **Properties** from the context menu. In the Properties dialog box, select the **Unblock** checkbox on the General tab, and click **OK** before running the installation kit again.

4. On the Welcome page, click **Next**.
5. On the View Notes page, click **Next**.
6. On the License Agreement page, read the license agreement. Select **I accept the terms of the license agreement**, and then click **Next**.
7. On the SQL Server Setup page, choose the SQL Server instance where the databases are installed. Select **SQL Server authentication**, enter SQL Server credentials, and then click **Next**.
8. On the Select Features page, select **Notification Service**, and then click **Next**.
9. On the Notification and Registration Configuration page, enter the IP address that the Proxy and Redirector will use to access the Notification service, and then click **Next**.
10. On the Notification Service – Locations and Virtual Directory page, specify the following Notification service information, and then click **Next**:
    - Installation location
    - Log file location. For security reasons, the log files should not be under the same path where the Notification service is installed.
    - Virtual Directory Name. Change this name if it will conflict with another already installed website/service. If you change the virtual directory name, record it. You will need to enter it when installing the proxy.
11. On the Services/Support Files page, specify the location for installing services and support files, and then click **Next**.
12. On the Machine Key File page, specify the location of the PortalKey.txt file that was copied to the server in Step 2. Click **Next**.
13. In the confirmation dialog box, click **Yes**.

    When the upgrade finishes, a Component Status page shows the version of each installed Portal component.
14. Click **Next**.
15. On the Upgrade Complete page, click **Finish**.

10 Upgrade Portal

For supported upgrade paths and system requirements, see the Portal release notes. Before you start the upgrade process, make sure that:

- Each system has the correct .NET and ASP.NET versions installed.
- There is enough free space for backing up the Portal databases. Portal databases are backed up automatically during an upgrade.

To upgrade Portal, do the following:

- Prepare for a Portal upgrade
- Upgrade Portal components
- Verify the upgraded Portal and make it available to users

If problems occur during an upgrade, you can roll back the Portal databases. See Roll back databases after a failed upgrade.

If you want to upgrade your operating system, we recommend upgrading Portal and then upgrading the operating system.

10.1 Prepare for a Portal upgrade

Before upgrading Portal, make sure that users cannot access the system, shut down services, and back up your databases.

Note: Before upgrading Portal, we recommend backing up Portal systems as described in Portal Disaster Recovery.

To prepare for a Portal upgrade:

1. Redirect the Login page to a “Site under maintenance page” to ensure that no users log in during the upgrade.
2. Check that the Portal UI is unavailable to the general public.
3. On each front-end system (i.e., server with the Portal UI installed):
   - Restart the IIS server to make sure that any users that are already logged in are logged out.
   - In a text editor, open the config file for the Portal Website (C:\inetpub\Portal Website\Web.config, by default). Look for the following lines:

     ```
     <location inheritInChildApplications="false">
       <system.web>
     ```

     In the location\system.web element, look for a machinekey line that is something like this:

```
<machineKey decryption="AES"
decryptionKey="6406C768ED214DD93F0EC68D5E18D0DA6FE4ABE44C588149
" validation="SHA1"
validationKey="E360EA1C515E2B9216AF500DF8EA2AA28C9418EA2F1B978B
CC6185E5075219B656A1E1EC6B2986DB9A8AC8B6BD370F547BC1A644C77B313
F8B35E456D8C37739" />
```

If a machineKey line appears in the location\system.web element, delete the entire machinekey line and then save the Web.config file. A machinekey entry in this element can cause problems during an upgrade.

4. On any server where Portal components are installed, shut down all Portal services.

   IMPORTANT: If you do not shut down the AMP Proxy and Redirector services before the upgrade, agents might not reconnect to Portal automatically after the upgrade.

5. Back up the EVaultWeb, WebCC, UserManagement, and SiteManagement databases.

10.2 Upgrade Portal components

To upgrade Portal components:

1. On each server where Portal components are installed, log in as an administrator and run the Portal installation kit.

   The Windows user must have full access to the Portal databases, or the upgrade might fail.

2. On the Welcome page, click **Next**.

3. On the SQL Server Setup page, choose the SQL Server instance where the databases are installed. Specify the authentication method, and then click **Next**.

   You can optionally click “Test” to validate your connection with the database server.

4. On any remaining installation wizard pages, provide the required information.

   Wizard pages that appear depend on the components that are being upgraded on the system. For information about specific pages, see Install Portal on a single system.

5. In the confirmation dialog box, click **Yes**.

   If a message states that sensitive information is now encrypted using the machine key, click **OK**. After the upgrade, be sure to back up the machine key file (usually named PortalKey.txt). If Portal front-end and back-end components are installed on the same server, back up the Host Protect web.config file (C:\inetpub\Portal Services Website\Host_Protect\web.config, by default).

   After Portal components are upgraded, a Component Status page appears. This page indicates which components have been installed and which components need to be installed before the system will be operational.

6. Click **Next**.

7. On the Upgrade Complete page, click **Finish**.
8. If you want to open a browser to the Portal sign in page, click **Yes** in the final message box.
9. Make sure that you have a backup copy of the Portal Website web.config file (C:\inetpub\Portal Website\web.config, by default) and keep the backup copy somewhere safe. You might need this file when converting Portal from a single system to a two-server distributed system or recovering Portal after a disaster.

10.3 Verify the upgraded Portal and make it available to users

To verify the upgraded Portal and make it available to users:

1. After upgrading Portal back-end and front-end components, verify that the Portal installation is functional. See Validate the Portal installation for the steps to do this.
2. Remove the redirection completed in Prepare for the Portal upgrade, and point to the login location previously used for Portal.

Note: After upgrading Portal, we recommend backing up Portal systems as described in Portal Disaster Recovery.

10.4 Roll back databases after a failed upgrade

During an upgrade, dump files are created. These can be used to manually roll back the databases in case the upgrade fails.

Databases are backed up to the following files:

- EVaultWeb.bak
- WebCC_database.bak
- UserManagement_database.bak
- SiteManagement_database.bak

Each dump file name also includes the date and time when the file was created. Dump files are typically saved in the following location: C:\WebCCDBBackup\

Dump files remain after an upgrade. You should periodically clean up the files.

The database files are not removed whether the upgrade succeeds or fails. They are not removed during uninstallation. They are not created or updated when a fresh Install, Repair, or Modify is run.

11 Validate the Portal installation

After installing Portal, check that the system is working by performing the following tasks:

- Log in to Portal for the first time
- Create a site
- Create an Admin user
- Add a computer
- Add a backup job
- View the Reports tab

11.1 Log in to Portal for the first time

A default super user is added when you install Portal. You can log in as this super user to start validating the installation.

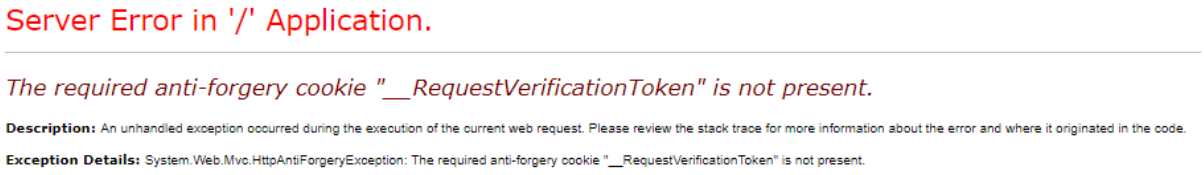
To log in to Portal for the first time:

1. In a supported Web browser, go to the Portal URL.
2. Log in using the default super user credentials:

   User Name = **super** Password = **3Vlt1nc**
3. In the **Change Password** dialog box, enter the super user's current password and new password, and then click **Change Password**.

   Note: The password is case-sensitive.

IMPORTANT: If the following server error appears when you try to log in to Portal, SSL use has not been configured correctly. You must either configure Portal to use SSL (recommended) or configure Portal to not use SSL. See Configure Portal SSL use.



11.2 Create a site

To create a site:

1. When logged in as the super user, click **Sites** on the navigation bar.
2. Click Create New Site.

   The **Site Details** tab opens.

3. In the Parent list, click **This site has no parent**.
4. In the **Site Name** box, enter a name for the new site. The site name must be unique.
5. (Optional) Enter other site information.
6. Click **Save Site**.

   The **Site Details** tab closes, and the new site appears in the grid.

11.3 Create an Admin user

Super users cannot add computers or manage backups in Portal. You must create an Admin user to ensure that you can perform these tasks in the new Portal installation.

To create an Admin user:

1. When logged in as the super user, click **User Manager** on the navigation bar.
2. Click **Create New User**.
3. On the **User Info** tab, in the **Email Address (Username)** box, type the user's email address.

   The user will log in to Portal using this email address.
4. In the **First Name** box, type the user's given name.
5. In the **Last Name** box, type the user's surname.
6. In the **Role** list, click **Admin**.
7. In the **Site** list, click the site that you created. See Create a site.
8. In the **Password** and **Confirm Password** fields, type the user's password for logging in to Portal.
9. Click **Create**.

11.4 Add a computer

To add a Windows, Linux or UNIX computer in Portal you must install or update Agent software on the computer. When asked to register the Agent with Portal, enter the host name that was entered when installing the externally accessible AMP Redirector Service. See Install the Proxy and Redirector for distributed systems, and Install Portal on a single system. For more information about registering an Agent with Portal, see the specific Agent guide.

To add a VMware vSphere 6.5 environment in Portal, install the vSphere Recovery Agent and register the Agent to Portal.

To add another supported vSphere environment, deploy a vSphere Agent and use the webcc register command to enter the Portal host name or IP address and port for communicating with Portal. For more information, see the *vSphere Agent User Guide*.

To add a Hyper-V environment in Portal, install a Hyper-V Agent and provide credentials for the agent to authenticate with a Hyper-V environment. For more information, see the *Hyper-V Agent User Guide*.

When adding a computer for Portal, you must enter the name of the Admin user you created. See Create an Admin user. The added computer appears on the Computers page when this user, or another Admin user for the site, logs in to Portal.

11.5 Add a backup job

To add a backup job:

1. In a supported Web browser, go to the Portal URL.
2. Log in as the Admin user you created. See Create an Admin user.
3. On the navigation bar, click **Computers**.
4. Find the computer that you added (see Add a computer), and expand its view by clicking the computer row.
5. If you are adding the first backup job for a Windows computer, click **Configure Manually**.
6. On the **Vault Settings** tab, click **Add Vault**. In the **Vault Settings** dialog box, enter vault information and credentials for connecting to the vault. Click **Save**.
7. Click the **Jobs** tab.
8. In the Select Job Task list, click Create New Local System Job.
9. In the **Create New Job** dialog box, specify the following information:
   - In the **Name** box, type a name for the backup job.
   - In the **Description** box, type a description for the backup job.
   - In the **Destination** list, select the vault where you want to save the backup data.
   - In the **Log File Options** list, select the level of detail for job logging.
   - If the **Encryption Settings** list appears, select an encryption method for storing the backup data.

- If the backup data will be encrypted, enter an encryption password in the **Password** and **Confirm Password** boxes. You can also enter a password hint in the **Password Hint** box.

10. In the **Select Files and Folders for Backup** box, select drives, folders, and files to include in the backup job.
11. Click **Create Job**.

    The job is created, and the **View/Add Schedule** dialog box appears. Click **Cancel** if you do not want to create a schedule.

11.6 View the Reports tab

To determine whether Server Backup EVault Reports is integrated with Portal, log in as an Admin user, and click the **Reports** tab.

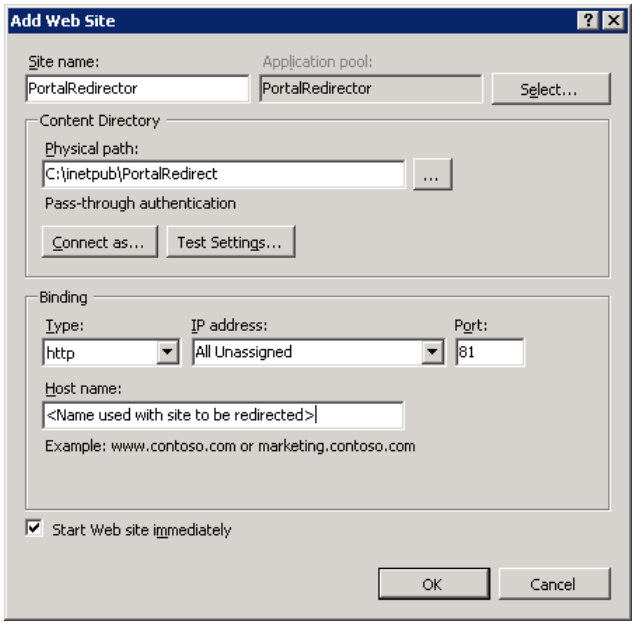
Reports only appear on the tab if Reports is integrated with Portal. See Integrate Portal with Reports.

12 Troubleshooting and Maintenance

This section describes issues that you might encounter when installing and managing Portal, and provides suggestions for resolving issues and maintaining Portal.

12.1 Redirecting Ports

- **Issue:** Portal was previously re-configured to use non-default ports, and users have bookmarks which use those non-default ports. After an upgrade to version 7.61 or later, the Portal website uses the default ports.
- **Solution:** Create a website which **listens** on the original (non-default) port and redirects the user to the default port
    - Open IIS Manager
    - Under “Sites” right click and “Add Web Site”
    - Configure the website as below:

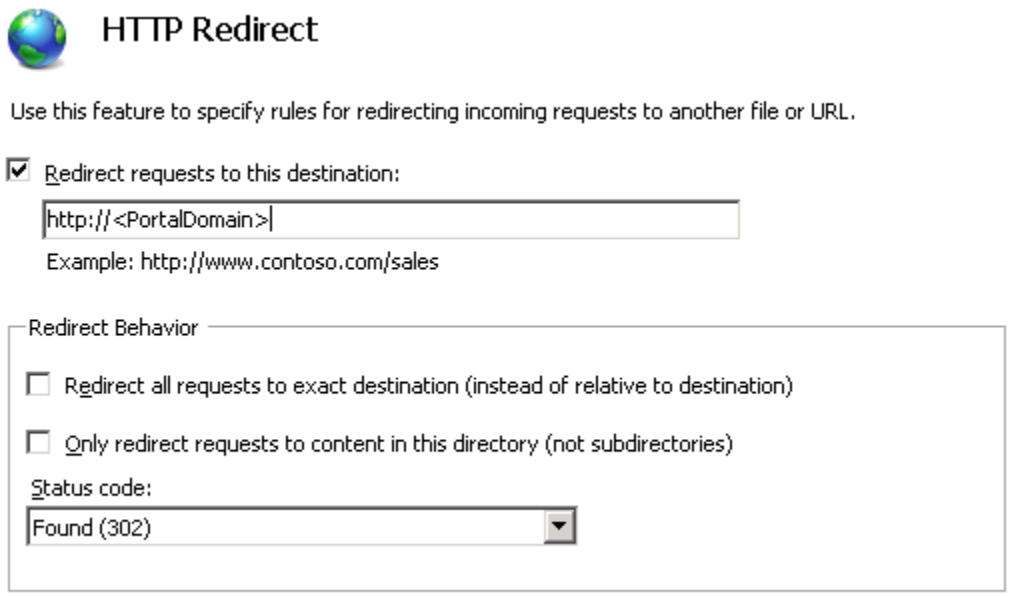


        - The **Physical Path** should point to a directory which has no other websites in it. It is recommended to create a new directory for this site.
        - The **Host Name** should be the name that was previously configured for the Portal website.
        - The **Port** should be the port that the website was previously configured under. Most likely, this would be port 81 or port 444 (if using https).
        - If using https, ensure that https is selected in the **Type** field.

- If your website was filtering based on IP address previously, provide that IP address under **IP Address**. Otherwise, leave as “All Unassigned”.

- Save the new website.
- Click on your newly added website and open the “HTTP Redirect” option from the features page.
  - If you do not see the “HTTP Redirect” option, you may have to install it. Refer to the following Microsoft site for how to install HTTP Redirect on your server:

    http://www.iis.net/configreference/system.webserver/httpredirect
- Provide the URL for the Portal. As it is now using default ports, there is no need to provide port information on the destination URL.



  - The destination should be the domain name for the Portal. Open your Portal application to get the domain name to use.

    Note: Do not include any sub directories or page information in this URL. It should go to the top level directory of your site (i.e., http://portal rather than http://portal/Account/LogOn?ReturnUrl=%2f).
- Verify that your redirection is working correctly by attempting to reach any page in the site that was being redirected.

  Note: This should be a temporary fix only. Users should be instructed to update their bookmarks to the new Portal URL.

12.2 SQL database installation failure

- **Issue:** SQL database installation fails with error: SQL instance is not a supported version.
- **Solution:** The problem could be permissions for the user on the database. The user you are installing the database under needs to have sysadmin access to master, model, msdb and tempdb databases. (DBOwner)

12.3 Agent doesn't register to Redirector

- **Issue:** Agent fails to register to Redirector
- **Solutions**:
    - Check Redirector logs first.
        - If error is related to database connection, verify that you have configured your database connection string correctly. If not, fix and restart the redirector
    - Verify that the Registration service is running
        - To verify if Registration service is working, go to IIS on the server where it is installed, go to the Registration web service application, content view, select the .aspx file that is there and right click/browse. If you see the list of API calls available, then the service is running.
    - Check that you have access to the Registration service from the redirector system.
        - Open the web.config file for the redirector and copy the URL configured there for the registration service. Open a browser on the redirector computer, paste in the URL and hit enter.
            - If you see the list of API calls available, then the service is running.
            - If not, you may not have the proper ports open between the redirector and the registration service. Redirector needs outbound access to port 80 for registration service and registration service needs inbound port 80 open from redirector.
    - Check that your agent can reach the Redirector
        - Could be firewalls in the way blocking access to the port
        - Check for both internal and external agents. In some cases, internal systems are not able to get out of the network to come back into the

DMZ, which means that external agents can register but internal ones cannot. Requires changes to the network configuration.

12.4 "Unauthorized proxy" errors

- Issue:
  - Errors in the notification service logs indicating "Unauthorized proxy"
  - Recent backup statuses are not being uploaded
  - Registrations are not succeeding
- Solutions:
  - Make the time consistent across all the systems in the configuration. (Proxies, backend server, front end server, etc).
  - Configuration problem:
    - In the Proxy configuration file, make sure the URl to the notification service is using an IP for connection.
      - In the proxy configuration file, make sure the same IP that is used in the URL for the notification service is set for the values for:
        `<add key="Proxy.WebService.Local.Address" value="" />`
        and
        `<add key="Proxy.Console.Listen.Address" value="" />`
    - In the notification configuration file, make sure the internal IP address is included in the list in the setting:
      `<add key="AMP.RemoteAddresses" value="127.0.0.1,localhost"/>`
    - Restart the proxy after fixing these issues.

12.5 Agents go offline sporadically

- **Issue:** Agents are dropping offline randomly for a few minutes at a time.
- **Solution:** Add another proxy to the configuration

12.6 Cannot load type when loading Portal login page

- **Issue:** In some cases, when a user tries to access the Portal login page, the login page does not load and the following message appears:

  ```
  Could not load type
  'System.ServiceModel.Activation.HttpModule' from assembly
  'System.ServiceModel, Version=3.0.0.0, Culture=neutral,
  PublicKeyToken=b77a5c561934e089'
  ```

- **Solution:** .NET Framework 3.x with Activation features is installed on the server. You must remove .NET version 3.x so that Portal will use .NET 4.x.
  - In IIS manager, click the machine name node.
  - In the Features view, double-click **Modules**.
  - In the list of modules, find **ServiceModel** and remove it.
  - Go back to the **machine name** node.
  - In the Features view, double-click **Handler Mappings**.
  - Find **svc-Integrated** and remove it.

12.7 NT AUTHORITY\SYSTEM login fails when navigating to Portal

- **Issue:** When Windows authentication is used for connecting to SQL server, and a user tries to navigate to Portal, a “login failed for NT AUTHORITY\SYSTEM” message appears.
- **Solution:** When Windows authentication is used, the sysadmin server role must be enabled for the NT AUTHORITY\SYSTEM login in the SQL Server instance where databases are installed. After the sysadmin server role is enabled for NT AUTHORITY\SYSTEM, restart SQL Server and the application pools.

12.8 403 error when attempting to open the Portal website

- **Issue:** When you open the URL that is configured for the Portal, you get a 403 error message.
- **Solution:** Ensure that the required .NET Framework versions are installed.

12.9 IIS default page appears instead of Portal sign-in page

- **Issue:** After an installation or upgrade, when you open the URL for the Portal, the default IIS page appears instead of the Portal. This occurs when IIS has cached its index page.

- **Solution:** Press F5 to refresh the browser when trying to view the Portal. This clears the browser cache, and Portal should appear.

12.10 Database transaction log files require monitoring

The recovery model for the Portal database, by default, is Full. Transaction logs can grow quickly and consume a significant amount of disk space.

Monitor the Portal database transaction logs to ensure that they do not grow unchecked. We recommend keeping transaction logs back to the last successful backup so that point-in-time recovery after the last backup is possible.

13 Portal Disaster Recovery

If you back up your Portal server or servers, you can recover the Portal instance, including all site, user and computer information

To back up and restore a distributed Portal instance, see Back up a distributed Portal instance, Restore SQL Server for a distributed Portal instance and Restore a distributed Portal instance.

To back up and restore Portal when all components are installed on a single system, see Back up Portal on a single system and Restore Portal on a single system.

13.1 Back up a distributed Portal instance

To back up a distributed Portal instance:

1. On each server where Portal components and/or the Portal SQL Server instance is installed, install the latest version of the 64-bit Windows Agent. Install the Image Plug-in with the Agent. Register each Windows Agent to the Portal instance that you are backing up.
2. For each server where Portal components are installed, create an Image job to protect the server. Include the **Entire Server** and **BMR** options in the Backup Set.
3. For the server where the Portal SQL Server instance is installed, create an Image job. Include the **Entire Server**, **BMR** and **Application Aware Backup – SQL Volumes Protected** options in the Backup Set.
4. Schedule the Image jobs created in Steps 2 and 3 to run. In a busy distributed instance, you could run the jobs several times per day (e.g., every four hours). In a Portal instance with less activity, you could run the jobs once per day.

IMPORTANT: Your backup data is safe, even if some Portal data is not backed up. Your backup data is stored in the vault, not in Portal.

13.2 Restore SQL Server for a distributed Portal instance

If the SQL Server database for a Portal instance has become corrupted, you can restore the SQL Server machine from a backup created in Back up a distributed Portal instance.

To restore the SQL Server database for a distributed Portal instance:

1. Using the System Restore application, restore the Portal SQL Server system from the Image job created in Step 3 of Back up a distributed Portal instance. For instructions, see the *System Restore User Guide*.
2. Sign in to Portal.

   Agents should be connected to Portal and Portal should be functioning properly.

13.3 Restore a distributed Portal instance

To restore a distributed Portal instance:

1. Using the System Restore application, restore the Portal SQL Server system from the Image job created in Step 3 of Back up a distributed Portal instance. For instructions, see the *System Restore User Guide*.
2. Restore any other servers where Portal components are installed from the Image jobs created in Step 2 of Back up a distributed Portal instance. For instructions, see the *System Restore User Guide*.

   IMPORTANT: When restoring a server where Portal back-end components are installed, be sure that the restored system has the same IP address as the original system.
3. Sign in to the restored Portal.
4. Do the following for each Portal server:

   a. On the Computers page, find the Portal server and view the Image job that protects the Portal server. Click **Synchronize** in the job's **Select Action** menu.

   b. Run the Image job that protects the Portal server.

      IMPORTANT: If the Image backup fails, delete the job folder and its contents on the server (by default, C:\Program Files\<*application*>\Agent*jobName*, where <*application*> is "OpenText Server Backup" for fresh Portal installs and "Carbonite Server Backup" for Portal instances that were upgraded from version 9.31 or earlier). Repeat Steps 2 to 3 to synchronize and run the Image job again. This might be required due to a known issue with some Windows Agent and System Restore versions.

13.4 Back up Portal on a single system

This procedure describes how to back up Portal when all Portal components and the Portal SQL Server instance are installed on the same system.

To back up Portal on a single system:

1. On the Portal server, install the latest version of the 64-bit Windows Agent. Install the Image Plug-in with the Agent. Register the Windows Agent to the Portal instance that you are backing up.
2. Create an Image Plug-in job to protect the Portal server. Include the **Entire Server** and **BMR** options in the Backup Set.

3. Schedule the Image Plug-in job to run. In a busy Portal instance, you could run the job several times per day (e.g., every four hours). In a Portal instance with less activity, you could run the job once per day.

IMPORTANT: Your backup data is safe, even if some Portal data is not backed up. Your backup data is stored in the vault, not in Portal.

13.5 Restore Portal on a single system

To restore Portal on a single system:

1. Using the System Restore application, restore the Portal system from the Image backup created in Back up Portal on a single system. For instructions, see the *System Restore User Guide*.

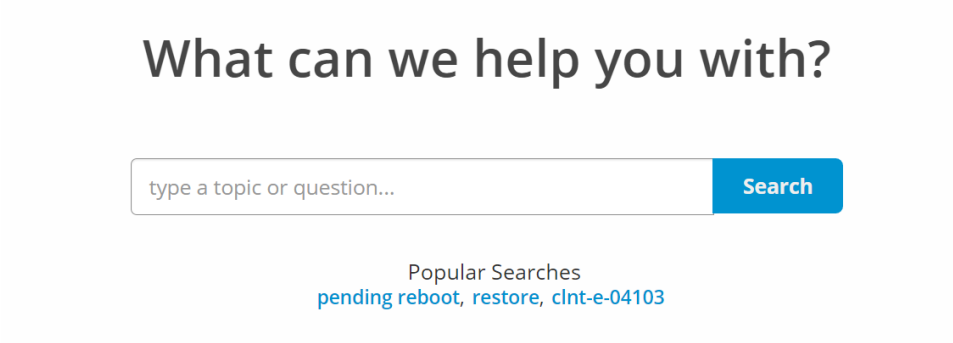
2. Sign in to the restored Portal. On the Computers page, find the Portal server and view the Image job that protects the Portal server. Click **Synchronize** in the job's **Select Action** menu.

3. Run the Image job that protects the Portal server.

   IMPORTANT: If the Image backup fails, delete the job folder and its contents on the server (by default, C:\Program Files\<*application*>\Agent*jobName*, where <*application*> is "OpenText Server Backup" for fresh Portal installs and "Carbonite Server Backup" for Portal instances that were upgraded from version 9.31 or earlier). Repeat Steps 2 to 3 to synchronize and run the Image job again. This might be required due to a known issue with some Windows Agent and System Restore versions.

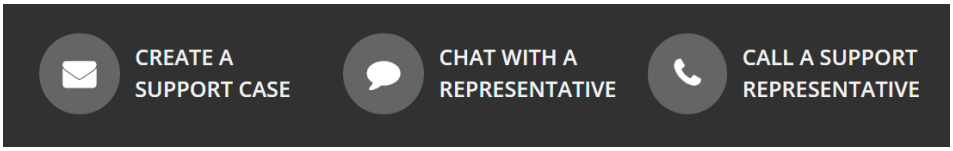
14 OpenText Server Backup Support

If you have a question about OpenText Server Backup that isn't covered in this guide, our frequently-updated Knowledge Base contains comprehensive information. The Knowledge Base is your first stop when searching for any OpenText Server Backup solutions you may need. We highly recommend searching here first for the quickest answers to your questions.



14.1 Contacting OpenText

If you need live assistance from a qualified support agent, OpenText Support is here for you 24 hours a day, 7 days a week (excluding US holidays). Please feel free to get in touch with us, and we'll help out any way we can! You can find the contact information for OpenText Support in the Knowledge Base.



Tip: When contacting Support with a technical issue, please have both the program's log files and the store you are having difficulty with ready.

To gather log files, click **File** menu and choose *Open log folder*. Compress the contents of the folder in a .zip file and attach it to your support request.

If the log archive and/or mail store exceeds 10MB, you may not be able to send them as an email attachment. In that case, upload instructions will be provided to you upon request.

Appendix A Configure single sign-on

By default, users are created in Portal and authenticated through a web form. However, users can be managed and authenticated using an external federated identity server (e.g., Active Directory Federation Services or Microsoft Entra ID). A Portal instance can use only one authentication method at a time: either Portal web form or federated identity server.

Important:

- If a Portal instance is configured to use Active Directory authentication, the configuration is permanent. You cannot change back to Portal web form authentication without recreating all user records in Portal.
- Child sites are not supported in Portal when a federated identity server is used to manage Portal users.
- Admin users and regular users who sign in using single sign-on credentials must enter Agent Registration passwords before they can register agents to Portal. For more information, see the *Portal User Guide* or Server Backup online help.
- If a user has been assigned the role of "Super" successfully through Active Directory, do not change the user's role to "Admin". If a change is required, please delete the user and then add the user again.

When a federated identity server is used, a user is directed to the external server for authentication. Once authenticated, the user is directed back to Portal with a SAML token. The token includes information from the identity server for automatically creating a user in Portal. This automatically-created user specifies the user's type and rights in Portal. It cannot be used to sign in to Portal.

Information for an automatically-created user in Portal is not necessarily up-to-date with information in the federated identity server. For example, if a user is deleted from Active Directory, the corresponding user is not automatically deleted from Portal.

The following requirements must be met for Portal single sign-on (SSO):

- The federated identity server must support WS-Federation (e.g., Active Directory Federation Services).
- Portal must be configured to use the federated identity server. See Configure Portal to use a federated identity server.
- The SAML token must contain all of the information required to automatically create or update the corresponding user in Portal. See Username in the SAML token, User role in the SAML token, User site in the SAML token, and SAML token/Expected claims.

This appendix describes how to:

- Configure single sign-on in Portal
- Configure single sign-on using Microsoft Entra ID
- Troubleshoot single sign-on

A1 Configure single sign-on in Portal

A1a. Configure Portal to use a federated identity server

To configure Portal to use a federated identity server, make the following changes in the Portal Web.config file:

- Disable forms authentication
- Enable federated authentication, which will handle incoming SAML tokens
- Configure identity provider settings

IMPORTANT: Other configuration changes may be required, depending on the identity server that you use.

To configure Portal to use a federated identity server:

1. Locate the Portal Web.config file. By default, this file is saved in c:\inetpub\Portal Website.
2. Open the Portal Web.config file in a text editor.
3. Disable forms authentication by doing the following:
   a. Locate the following lines:

```
<authentication mode="Forms">
    <forms loginUrl="~/Account/LogOn" timeout="30" />
</authentication>
```

   b. Replace the lines shown above with the following lines:

```
<authentication mode="None" />
<authorization>
    <deny users="?" />
</authorization>
```

4. Enable federated authentication by doing the following:
   c. Locate the <add name="HttpResponseHeaderSanitizer"…> line or lines.

      This line could appear more than once in the Web.config file.

d. Directly after each occurrence of the <add name="HttpResponseHeaderSanitizer"…> line, add the following lines:

```
<remove name="FormsAuthentication" />
<add name="WSFederationAuthenticationModule"
type="EVault.Web.UI.WSFederationAuthentication,
EVault.Web.UI" preCondition="managedHandler" />
```

5. Configure identity provider settings by doing the following:

a. Locate the </configuration> line.

b. Directly before </configuration> line, add the following section:

```
<system.identityModel>
    <identityConfiguration>
      <claimsAuthenticationManager
type="EVault.Web.UI.HttpModules.ClaimsTransformerWrapper,
EVault.Web.UI"/>
      <audienceUris>
        <add value="yourAudienceUri" />
      </audienceUris>
      <certificateValidation
certificateValidationMode="ChainTrust" />
      <issuerNameRegistry
type="System.IdentityModel.Tokens.ValidatingIssuerNameRegistry,
System.IdentityModel.Tokens.ValidatingIssuerNameRegistry">
        <authority name="yourIssuerSiteId">
          <keys>
            <add
thumbprint="yourIssuerSigningCertificateThumbprint" />
          </keys>
          <validIssuers>
            <add name="yourIssuerSiteId" />
          </validIssuers>
        </authority>
      </issuerNameRegistry>
    </identityConfiguration>
  </system.identityModel>
  <system.identityModel.services>
    <federationConfiguration>
     <cookieHandler requireSsl="true" />
      <wsFederation passiveRedirectEnabled="true"
issuer="yourIssuerUrlPassiveRedirectionUri"
realm="yourAudienceUri" requireHttps="true" />
```

```
    </federationConfiguration>
</system.identityModel.services>
```

c. Replace the highlighted variables with the appropriate values for your environment:

- yourAudienceUri is the Portal installation URI.
- yourIssuerUrlPassiveRedirectionUri is the passive requestor URL of your identity provider. This value can be found in the federation metadata in the following element: PassiveRequestorEndpoint/Address
- yourIssuerSiteId is the configured URI of the issuer sent within SAML token (sometimes referred to as "Site ID"). This value can be found in the federation metadata in the entityID attribute of the EntityDescriptor element.
- yourIssuerSigningCertificateThumbprint is the IdP signing certificate thumbprint. It must be entered in uppercase with no dashes (e.g., "886B8DC3498FF93A8D0B844DC2F9085116E7EE51"). The IdP signing certificate must be installed on any machine where the Host Protect Service is installed. See Install IdP Signing Certificate on the machine where Portal is installed.

6. If you are using a self-signed certificate for testing, disable certificate revocation checking by doing the following:

   a. Locate the <certificateValidation line added in Step 5:

   ```
   <certificateValidation certificateValidationMode="ChainTrust" />
   ```

   b. Replace the line shown above with the following line:

   ```
   <certificateValidation certificateValidationMode="ChainTrust"
   revocationMode="NoCheck" />
   ```

7. Save the Portal Web.config file.

A1b. Install IdP Signing Certificate on the machine where Portal is installed

For Portal single sign-on, the Identity Provider signing certificate must be installed on the machine where Portal is installed.

If Portal is installed as a distributed system, the certificate must be installed on each machine where the Host Protect Service is installed.

A1c. Username in the SAML token

The username will be retrieved from the following attribute in the SAML token:

```
AttributeName="username"
AttributeNamespace="http://company.com/identity/claims/portal"
```

The suggested formats for username are:

- User Principal Name (UPN) - e.g., user@domain.com
- User Logon Name - e.g., user
- Windows Account Name - e.g., domain\user

Note: For the *company* value in each claim, please contact Support.

Due to Agent limitations, it is best to avoid spaces and apostrophes in user names. For this reason, the UPN format is recommended.

To ensure compatibility with the single sign-on implementation in Portal versions 7.70 and 7.62, if the "username" attribute is not present, the username should be retrieved from the following attribute: `EVaultPortalUserName`

This attribute can be present in any namespace.

If this attribute is not present, use the default name attribute:

```
AttributeName="name"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
```

A1d. User role in the SAML token

A user's role in Portal can be determined based on group membership or another Active Directory schema attribute. A customer can use their existing group structure, and map their existing (or new) roles to a specific portal claim, using ADFS claim transformation. The benefit of this approach is that when using proper federation with many external issuers (components that actually authenticate users), and a single federation provider (component that generates final SAML token for Portal), the transformation can be done in one place (federation provider) rather than requiring the same schema for every issuer.

Here is a working example of a claim as passed in the SAML token to Portal:

```
<saml:Attribute AttributeName="role"
AttributeNamespace="http://company.com/identity/claims/portal">
     <saml:AttributeValue>SuperUser</saml:AttributeValue>
     <saml:AttributeValue>Support</saml:AttributeValue>
   </saml:Attribute>
```

In this case, two roles are passed to Portal. If multiple roles are passed, Portal will pick the most-privileged role.

Note: For the *company* value in each claim, please contact Support.

A1e. User site in the SAML token

The current single sign-on implementation is not intended for Portal instances with many sites. However, because there could be more than one site in a Portal instance, the SAML token for a user must include a site identifier. When a user signs in to Portal, the identifier will be matched with the existing site name in Portal to retrieve its ID.

Note: Site names must be pre-populated in Portal.

```
<saml:Attribute AttributeName="sitename"
AttributeNamespace="http://company.com/identity/claims/portal">
<saml:AttributeValue>Data Factory Company</saml:AttributeValue>
</saml:Attribute>
```

Note: For the *company* value in each claim, please contact Support.

The alternate way to provide this information would be to provide the siteid attribute:

```
<saml:Attribute AttributeName="siteid"
AttributeNamespace="http://company.com/identity/claims/portal">
<saml:AttributeValue>22EFA16B-32D8-4904-9C70-
EFCDAAF38F02</saml:AttributeValue></saml:Attribute>
```

If present, this attribute will take precedence and override any value passed in a sitename claim. It safer to use the siteid attribute than the sitename attribute, as those IDs are unique and less likely to change.

A1f. SAML token/Expected claims

This section lists the claims that Portal will expect in the SAML token.

Note: For the *company* value in each claim, please contact Support.

Username

This is the user name. It could be in email address format (UPN), but it can also be logon name (username) or windows account name (domain\username)

```
AttributeName="username"
AttributeNamespace="http://company.com/identity/claims/portal"
```

Here is sample claim transformation rule for UPN name:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windows
accountname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types =
("http://company.com/identity/claims/portal/username"), query =
";userPrincipalName;{0}", param = c.Value);
```

User Id

This is the unique, non-changing identifier of the user.

```
AttributeName="userid"
AttributeNamespace="http://company.com/identity/claims/portal"
```

If the same value is passed in as username, it will be impossible to change the user name without losing the user identity. (Anew user would be created in Portal). It is suggested to use LDAP objectGuid property for this claim. Here is the example of that rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windows
accountname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types =
("http://company.com/identity/claims/portal/userid"), query =
";objectGuid;{0}", param = c.Value);
```

First name

This is the user first name:

```
AttributeName="firstname"
AttributeNamespace="http://company.com/identity/claims/portal"
```

Last name

This is the user last name:

```
AttributeName="lastname"
AttributeNamespace="http://company.com/identity/claims/portal
```

Name

This is the username. This is standard claim, and is sometimes passed by the federation provider without the ability to be overwritten by the username in email format. For this reason, this claim will be used only if the username claim above is not provided.

This claim is optional and is processed for backwards compatibility only. If provided, this should correspond to the AD UPN name (email format).

```
AttributeName="name"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identi
ty/claims"
```

Role

This claim can contain a value from the following list:

- SuperUser – Super users can add and manage sites and users in Portal. However, Super users cannot add or manage companies, create or run backup jobs, or run restores. Super users can only view pages in Portal that are used for managing sites and users.

Super users are associated with company ID 00000000-0000-0000-0000-000000000000.

- SupportUser – Support users can view information and reports for all sites in Portal. However, Support users cannot add or manage computers, create or run backup jobs, or run restores. Support users are associated with company ID 00000000-0000-0000-0000-000000000000.
- Admin – Admin users in a site can create and manage users, and access all computers associated with users in a site. Admin users can add computers, delete offline computers, create and run backup jobs, and run restores. Admin users can also create policies and run reports. An Admin user is associated with a specific company ID.
- User – Users in a site can add computers, create and run backup jobs, and run restores. Users can only access computers that they added or that are assigned to them in the site. A user is associated with a specific company ID.
- ExecuteOnly – Execute-only users can run existing jobs and view logs. However, these users cannot create, edit or delete anything in Portal. An Execute-only user is associated with a specific company ID.
- ReadOnly – Read-only users can only view certain logs, statuses and reports in Portal. A Read-only user is associated with a specific company ID.

```
AttributeName="role"
AttributeNamespace="http://company.com/identity/claims/portal"
```

This claim can be populated by list of claim transformation rules that will set up given roles based on AD group membership, for example:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsi
d", Value == "S-1-5-21-2234195498-1907527747-1912965387-1107",
Issuer == "AD AUTHORITY"]
=> issue(Type =
"http://company.com/identity/claims/portal/role", Value =
"SuperUser", Issuer = c.Issuer, OriginalIssuer =
c.OriginalIssuer, ValueType = c.ValueType);
```

Site name

This claim contains the user's site name:

```
AttributeName="sitename"
AttributeNamespace="http://company.com/identity/claims/portal"
```

When there is only one site, this value can be hardcoded in the claim transformation rule to the active site. For example:

```
=> issue(Type =
"http://company.com/identity/claims/portal/sitename", Value =
"Big Data Company");
```

Site Id

This optional claim contains the site GUID for the user site. If present, this will take precedence over site name, allowing more secure user to site association.

```
AttributeName="siteid"
AttributeNamespace="http://company.com/identity/claims/portal"
```

Here is an example of usage:

```
=> issue(Type =
"http://company.com/identity/claims/portal/siteid", Value =
"B0ADAD3F-D66A-4078-97A0-2C0BB14A4942");
```

User auto-provisioning

This claim specifies whether the user is external to Portal and therefore if auto-provisioning should happen or not. The possible values would be “true” and “false”. If the claim is not present, auto-provisioning will be disabled. This is provided for backwards-functionality. For new customers, this claim should always be passed as True:

```
AttributeName="isuserexternal"
AttributeNamespace="http://company.com/identity/claims/portal"
```

Here is a sample claim transformation rule:

```
=> issue(Type =
"http://company.com/identity/claims/portal/isuserexternal",
Value = "true");
```

A2 Configure single sign-on using Microsoft Entra ID

This section describes how to configure Portal single sign-on using Microsoft Entra ID (formerly known as Azure Active Directory).

IMPORTANT: Procedures for Microsoft Entra ID may change. For current information and procedures, see documentation from Microsoft.

A2a. Prerequisites

- A Portal system where you have logged in at least once as the built-in Super user.
- Portal is hosted on port 443 (https).

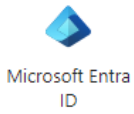
- At least one site in Portal where users can be auto-provisioned. In examples in this appendix, the site name is ParentSite1.
- An Azure account that can edit Entra ID items, and create Enterprise applications, users and groups in the target Entra ID directory.

A2b. Set up groups and users in Entra ID

In Entra ID, you must create groups of users who will be able to sign in to Portal.

To set up groups and users in Entra ID:

1. Sign in to the Microsoft Azure portal.
2. Go to **Microsoft Entra ID**:



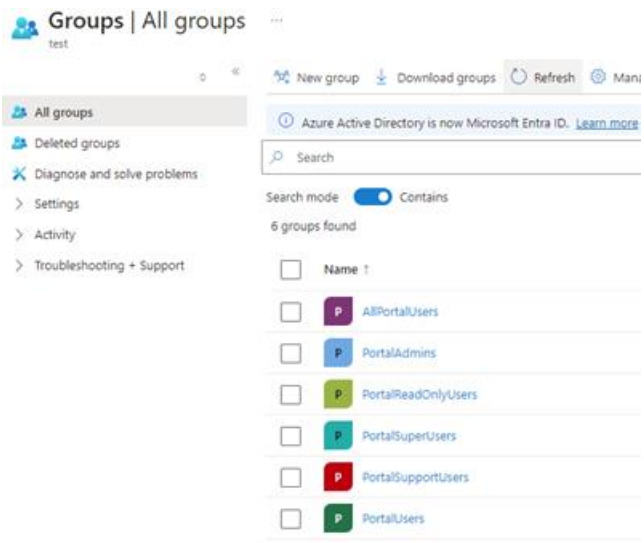
3. Create a group that will contain all Portal users and groups. The group should have the “Security” group type.

   For example, the name of the group could be “AllPortalUsers”.

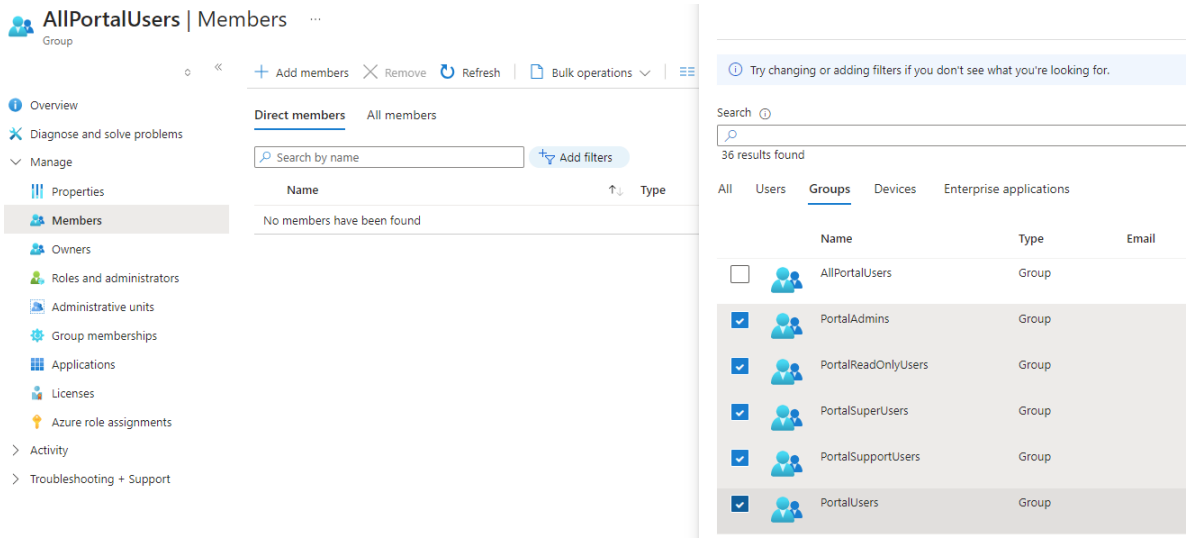
4. Create five groups that will map to the Portal user types. The groups should have the “Security” group type.

   For example, the group names could be:

   - PortalAdmins
   - PortalReadOnlyUsers
   - PortalSuperUsers
   - PortalSupportUsers
   - PortalUsers



5. Add the five groups that will map to the Portal user types created in Step 4 to the group for all Portal users and groups created in Step 3.



6. In Entra ID, create any Portal users that you want. At a minimum, you must have a Super user and either an Admin or regular user who can register agents.

- *Note:* Admin users and regular users who sign in using single sign-on credentials must enter Agent Registration passwords before they can register agents to Portal. For more information, see the *Portal User Guide* or Server Backup online help.

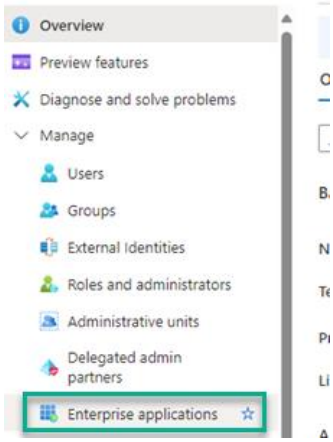
7. Assign each user created in Step 6 to the appropriate Portal user type group created in Step 4.

A2c. Create an enterprise application in Entra ID

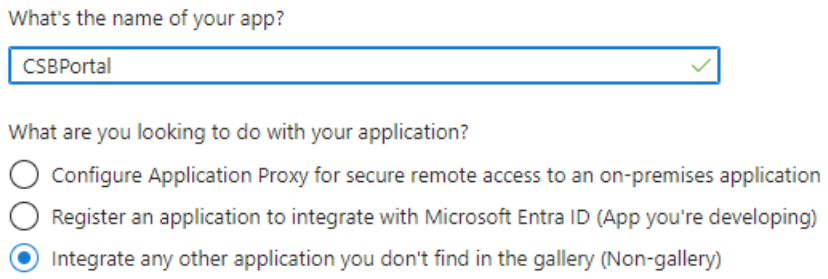
To configure single sign-on with SAML tokens, you must create an enterprise application in Entra ID.

To create an enterprise application in Entra ID:

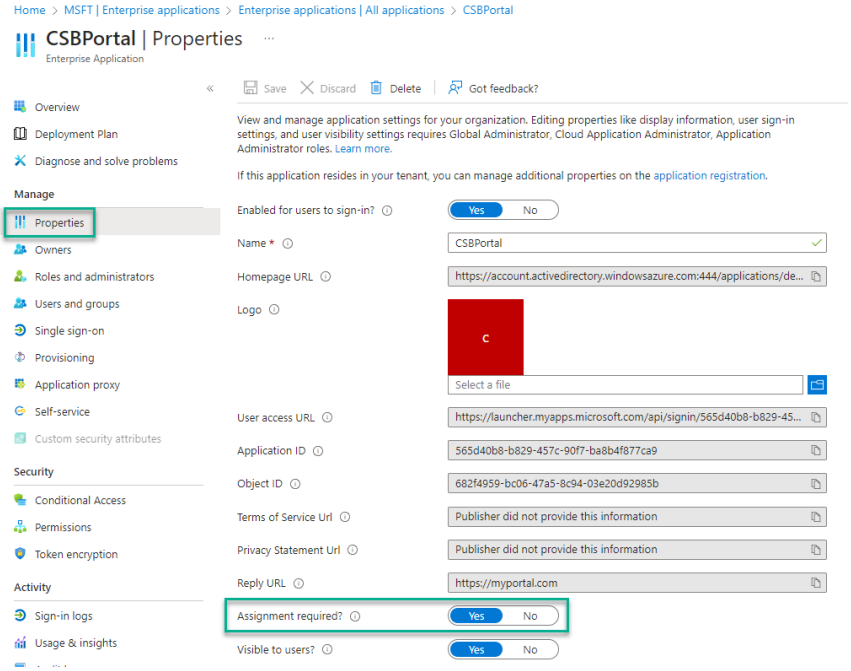
1. In Entra ID, go to **Manage** > **Enterprise applications**.



2. Click **New application**.
3. Click **Create your own application**.
4. In the **Create your own application** pane, enter a name for your application (e.g., CSBPortal) and select **Integrate any other application you don't find in the gallery (Non-gallery).** Click **Create**.



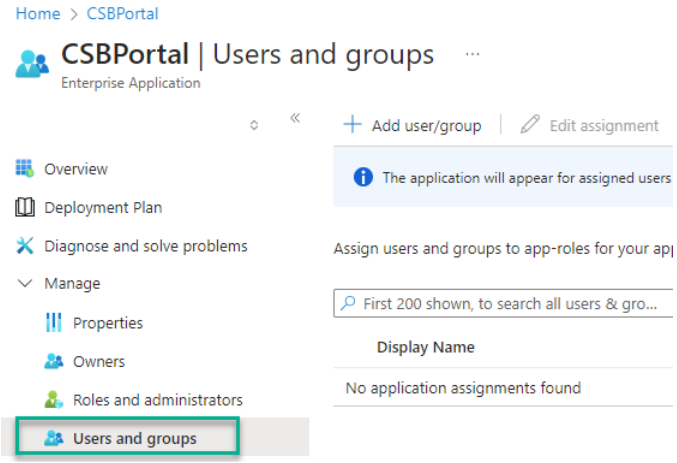
5. After the application is created, go to **Manage** > **Properties**.



6. On the Properties page for the application, do one of the following:

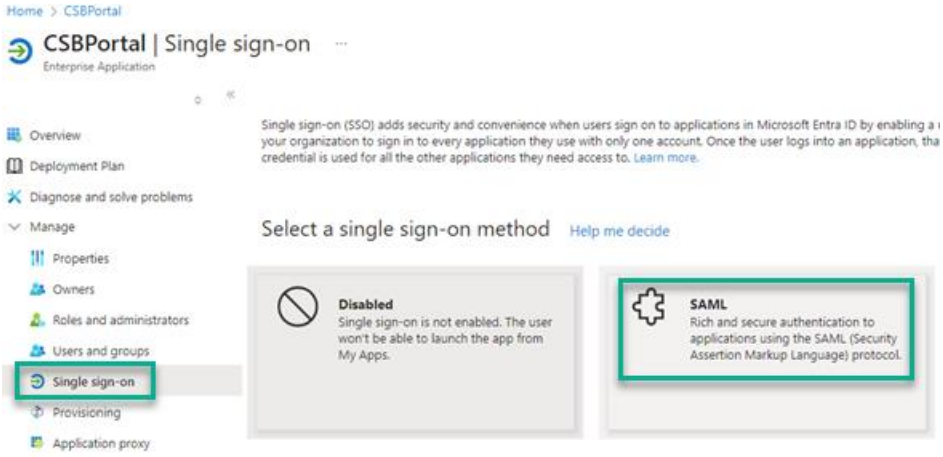
   - To specify that all users in your organization can sign in to Portal, set the **Assignment required** switch to **No**, and then click **Save**.
   - (Recommended for increased security) To specify that users and groups must be assigned to the Portal application to be able to sign in to Portal, set the **Assignment required** switch to **Yes**, and then click **Save**.

     Go to **Manage** > **Users and groups**. Assign the group that contains all Portal users and groups to the application (e.g., named "AllPortalUsers").



Note: If a *Groups are not available for assignment due to your Active Directory plan level* message appears, you cannot assign groups to the application. Instead, you must assign individual users to the application.

7. Go to **Manage** > **Single sign-on**. Click **SAML**.



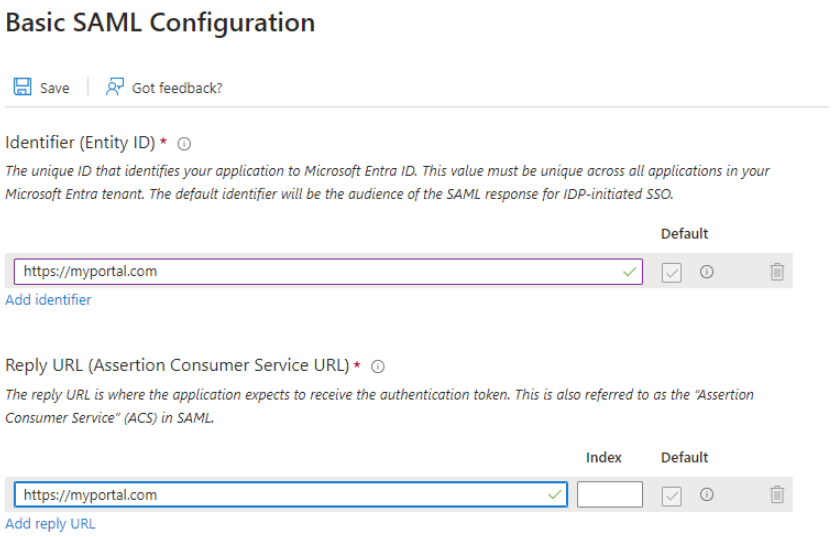
8. On the **SAML-based Sign-on** page, in the **Basic SAML Configuration** box, click **Edit**. In the **Basic SAML Configuration** pane, do the following:

   a. In the **Identifier (Entity ID)** box, type an identifier. The identifier can be any value but is typically the Portal URL (e.g., https://myportal.com).

      Note: If this text box is not available, click **Add identifier** to display the box.

   b. In the **Reply URL (Assertion Consumer Service URL)** box, type the address of the Portal (e.g., https://myportal.com).

      Note: If this text box is not available, click **Add reply URL** to display the box.



c. Click **Save**.

d. Close the **Basic SAML Configuration** pane.

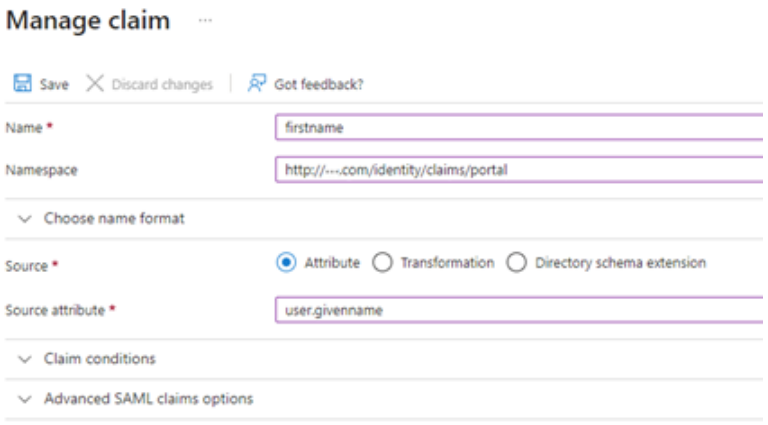
9. In the **Attributes & Claims** box, click **Edit**. On the **Attributes & Claims** page, add each claim shown in the following table. To add a claim, do the following:

   a. Click **Add new claim**.

   b. On the **Manage claim** page, type the Name and Namespace values, and select or type the Source attribute value.

      Note: Each name must be written in lowercase letters only (i.e., no uppercase).

   c. Click **Save**.



Name	Namespace	Source attribute
firstname	http://*company*.com/identity/claims/portal	user.givenname
isuserexternal	http://*company*.com/identity/claims/portal	true *You must type* true*. It then appears in quotation marks in the claims list.*
lastname	http://*company*.com/identity/claims/portal	user.surname
sitename	http://*company*.com/identity/claims/portal	*Site name in Portal* (e.g., ParentSite1) *You must type the site name. It then appears in quotation marks in the claims list.*
userid	http://*company*.com/identity/claims/portal	user.userprincipalname
username	http://*company*.com/identity/claims/portal	user.userprincipalname
role	http://*company*.com/identity/claims/portal	*Instead of entering a value in the Source attribute box, set up claim conditions as described in the following step.*

Notes:

- For the hardcoded *company* value in each claim, please contact Support. This value is only available from Support.
- You may get a warning that certain names are protected. You can ignore this because the name space is non-standard.

10. For the role claim, click **Claim conditions** on the **Manage claim** page to expand the section, and add five conditions: one for each Portal user type. These conditions ensure that users have the correct role when they sign in to Portal. To add a condition, do the following:

    a. In the **User type** list, select **Members**.

    b. In the **Scoped Groups** column, click **Select groups**. In the group list, select a group that maps to a Portal user type (e.g., PortalSuperUsers). These groups were created in Step 4 of Set up groups and users in Entra ID. Click **Select**.

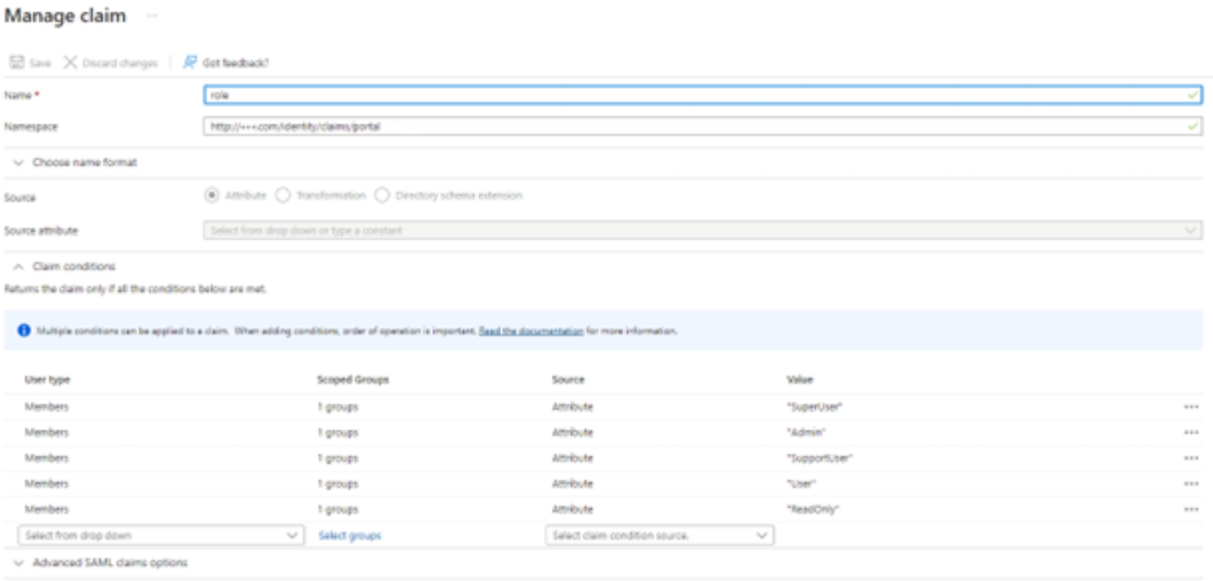
    c. In the **Source** list, select **Attribute**.

    d. In the **Value** column, enter the Portal user type that corresponds to the group selected in the **Scoped Groups** column:

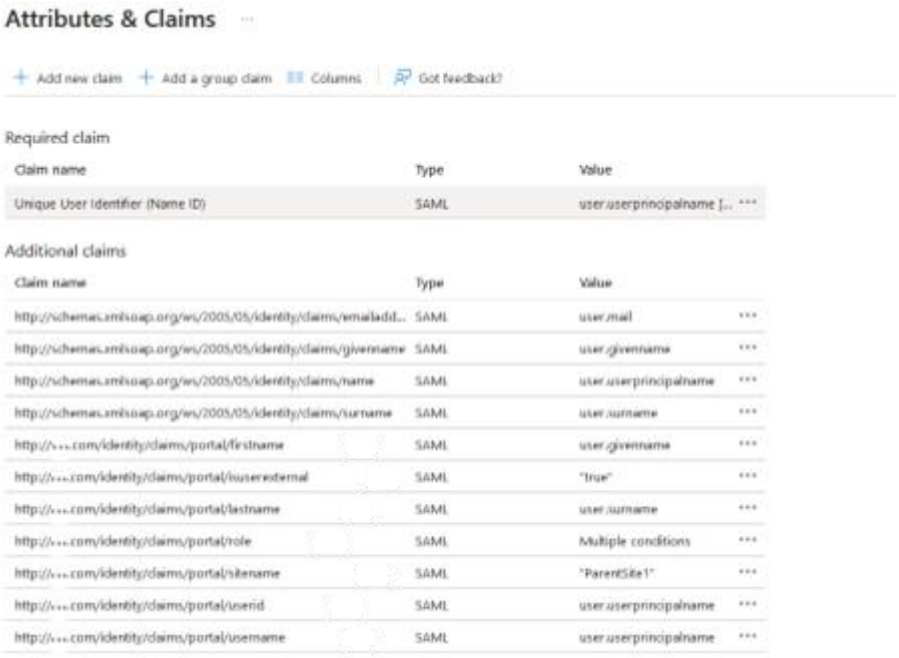
        - SuperUser
        - SupportUser
        - Admin
        - User
        - ReadOnly

After creating the claims, click **Save**.

The resulting **Manage claim** page should look like the following:



After adding all claims, the **Attributes & Claims** page should look something like the following:



A2d. Set up certificate and configuration values

To set up certificate and configuration values:

1. On the **SAML-based Sign-on** page for the application, in the **SAML Certificates** box, do the following:

    a. Click the **Certificate (Base64) Download** link.

    You must install the downloaded certificate as a trusted root certificate on all Portal machines with the Host Protect Service. If all Portal components are installed on one server, install the downloaded certificate only on that one machine.

    b. Copy the **Thumbprint** value and record it somewhere. You will need the certificate thumbprint value when configuring the Portal Web.config file.

    c. Click the **Federation Metadata XML** download link. You will need values from the downloaded XML file when configuring the Portal Web.config file.

2. In the **Set up *applicationName*** box (e.g., **Set up CSBPortal**), copy the **Login URL** and **Microsoft Entra Identifier** values and record them somewhere.

3. Configure Portal. Update the Portal Web.config file as described in Configure Portal to use a federated identity server using the following values:

    - yourAudienceUri = the application ID you entered in Step 8a of Create an enterprise application in Entra ID. The application ID is typically the Portal URL (e.g., `https://myportal.com`).

    - yourIssuerUrlPassiveRedirectionUri = the passive requestor URL of your identity provider. This value can be found in the Federation Metadata XML file that you downloaded in Step 1c, in the following element: PassiveRequestorEndpoint/Address (e.g., `https://login.microsoftonline.com/999910b6-9987-413d-a986-99991924ed3a/wsfed`).

    - yourIssuerSiteId = the Microsoft Entra Identifier that you copied in Step 2 (e.g., `https://sts.windows.net/999910b6-9987-413d-a986-99991924ed3a/`).

    - yourIssuerSigningCertificateThumbprint = the certificate thumbprint value that you copied in Step 1b.

4. Visit your Portal website. You should be redirected to login.microsoft.com to log in with your Entra ID (Azure AD) credentials. After login, you should be redirected to Portal.

    Support and Super users should be auto created in Portal, and site-level users should be created in the site configured in the sitename claim (e.g., ParentSite1).

A3 Troubleshoot single sign-on

Issue 1: After logging off Portal, the ADFS sign-out page appears. However, if the Portal URL is entered again without restarting the browser, the user is automatically logged in again. Why does this happen?

Answer: Even though all authentication cookies are cleared properly, this happens because the browser caches authentication credentials to ADFS until the browser is restarted. This can be verified by investigating sent headers with Firebug - notice the Authorization NTLM header being sent.

You can also manually clear authentication credentials in Firefox by pressing Ctrl+Shift+Del and choosing “Active Logins”. This will force ADFS to reauthenticate. In normal operating scenarios, we recommend that users should close the browser after logging off ADFS to ensure that credentials are not cached.

Issue 2: When trying to sign in to Portal, an error page appears. The logs state that the problem occurs because of a “username that already exists”.

Answer: This could occur if a user with the same name was already created for use with forms authentication (Portal web form authentication), or if a user with the same name was set up for federated authentication (external user) but with a different external user id. If the original user is no longer needed, it can be deleted by the super user. The new user will then be able to login successfully. Alternatively, the new user’s username can be changed to avoid duplication.

Issue 3: When trying to sign in to Portal, an error page appears with “An error occurred. Please click the link below and send the emails to support”. The logs state that the problem occurs because “Users cannot delete themselves”.

Answer: This could occur if the user has been created but the user’s role or company has changed. Instead of changing a user’s role, remove the user from Portal then log in again. This will force Portal to auto-provision the user as a new user instead of updating the existing user.