Manuals+ — User Manuals Simplified.

Changepoint API Software Installation Guide

API Installation Guide
Reference Guide
Changepoint 2021

Contents

Installing the Changepoint API

About installing the Changepoint API

The Changepoint API is available as a COM API, a Windows Communication Foundation (WCF) service and, for backwards compatibility, as a Web Services Enhancements (WSE) service. For information about the

Changepoint API, see the Changepoint API Reference. For upgrade notes, caveats and known issues, see the Release Notes in team folders in Changepoint.

Upgrading the Changepoint API

If you are upgrading from a previous release of Changepoint, use the Windows Control Panel to uninstall the previous version of the Changepoint API and its components before installing this version.

Changepoint API requirements

You must install Changepoint before you install the Changepoint API. For software requirements, see the Changepoint Software Compatibility Matrix, which is available in the 2021 Release Notes and Patches team folder in Changepoint.

File path conventions

Throughout this document, the following conventions are used for common paths:

- <cp_root> The root path of the Changepoint installation.

  The default path is:

  C:Program Files (x86)ChangepointChangepoint

- <cp_common> The root location for common Changepoint utilities, such as the Login Settings utility.

  The default path is:

  C:Program Files (x86)Common FilesChangepointChangepoint

Installing the Changepoint API

1. From the Changepoint API media root directory, run setup.exe.

2. Follow the prompts until the Select Features screen appears.

3. Select the features that you want to install, then click Next.

4. Select the API destination folder, default <cp_root>API, and click Next.

   Note: The Changepoint Login Settings utility is installed in <cp_common>LoginSettings, regardless of the destination folder that you specify.

5. If you selected the Web Services API: a. When the Select

   a Web Site screen appears, select a website to add the virtual directory to, and then click Next.

   b. Click Next to continue. 6. When the installation of the API is complete, click Finish.

Configuring the Changepoint API to be cache aware

To configure the Changepoint API to be cache-aware, replace the values for the "cache. Password" and "cache. Servers" keys in the CP Web ServicesWeb.config file with the values used in the EnterpriseWeb.config file.

Enabling Web Services Enhancements (WSE)

1. Edit the Web.config file for web services. The default location is:

   <cp_root>APICP Web ServicesWeb.config

2. Find the three instances of the following comment line:

   < !– Uncomment the following element if you are using Web Service Enhancements (WSE) API. Leave

   comments if using WCF services and are not installing Web Service Enhancements (WSE) –>

3. Uncomment the element that follows each instance of the comment line:

   <section name="microsoft.web.services2″ … > <webServices> <microsoft.web.services2>

   Note: The <webServices> element to be uncommented is a child of <system.web>.

Configuring logging for the Web Services API

You must set the log file path and log levels. The log levels are cumulative. For example, if you specify level 3, then levels 1, 2, and 3 are logged. The default log level is 8.

1. Edit the web services Web.config. The default location is:

   <cp_root>APICP Web ServicesWeb.config

2. Set the LogFilePath. The default value is <cp_root>APIAPILogs. 3. Set the LogLevel. The valid values are:

   0 = No logging

   1 = Source object and method

   2 = Error message

   3 = Input parameters

   4 = Returns

   5 = Warning

   8 = Checkpoint

Configuring virtual directory authentication for the Web Services API
You must enable anonymous access and disable Integrated Windows authentication for the CPWebService virtual directory in Internet Information Services (IIS). For more information, see the Microsoft IIS documentation.
Configuring database connection settings for the Web Services API
Use the Login Settings utility to encrypt the database connection settings in the Web Services API Web.config file. For more information, search for "Configuring Database Connection Settings" in the Changepoint Installation Guide.
Configuring authentication for Changepoint WCF Web Services
You can configure Application Authentication and single sign-on (SSO) for Changepoint WCF Web Services.
The following implementation options are available using Secure Token Service (STS):

- SSO using ISAPI SSL optional
- SSO using WS-Federation (ADFS 2.0) SSL required

If SSL is required, the configuration script ensures that it is used.
The configuration scripts for ISAPI and application authentication can optionally enable SSL.
Configuring application authentication for WCF Web Services
The default authentication type for Changepoint WCF Web Services is application authentication.
Use the procedures in this section to:

- configure Changepoint WCF Web Services to use application authentication with SSL
- revert Changepoint WCF Web Services to application authentication after having implemented one of the SSO implementations

Configure PowerShell

1. Open a Windows PowerShell prompt.
2. Modify the execution policy:

   Set-ExecutionPolicy Unrestricted

Stage 1 Collect configuration parameters
Determine the values for the configuration parameters.

Parameter	Description
WebService_Path	Location of the Changepoint WCF Web Services web application files. Default: <cp_root>\API\CP Web Services
ServiceCertificate_ Name	Certificate name that will be used to authenticate the service to clients using Messa ge security mode. Default: the "CN=ChangepointAPICertificate" Certificate Name.
require HTTPS	Require HTTPS (True/False) Default: False.

Stage 2 Execute configuration scripts

Use the values for the configuration parameters to modify the configuration of the websites.

1. Open a PowerShell prompt.

   Note: If your server has User Account Control enabled, you must open the PowerShell prompt using elevated

   administrator permissions.

2. Navigate to the CP web service configuration directory, default:

   <cp_common>ConfigurationCPWebService

3. Execute ./Configuration_AppAuth.ps1

4. Follow the prompts.

Configuring single sign-on (SSO) for WCF Web Services
Configure PowerShell

1. Open a Windows PowerShell prompt.

2. Modify the execution policy:

   Set-ExecutionPolicy Unrestricted

Configuring SSO using ISAPI for WCF Web Services
Stage 1 Collect configuration parameters

Determine the values for the following configuration parameters.

Parameter	Description
WebService_Path	The location of the Changepoint WCF Web Services web application files. Default: <cp_root>\API\CP Web Services
require HTTPS	Require HTTPS (True/False). Default: False.
Changepoint_RSA_ Cookie_Transform	The name of the certificate that you use for Cookie encryption. Default: the "CN=ChangepointAPICertificate" Certificate Name.
ServiceCertificate_Nam e	Enter the certificate name that will be used to authenticate the service to clients using Message security mode. Default: the "CN=ChangepointAPICertificate" Certificate Name.
SigningCertificate_Nam e	Enter the signing certificate name. This is the name of the certificate that you use for signing messages. Default: the "CN=ChangepointAPICertificate" Certificate Name.
ISAPI_Mode	The ISAPI mode. Default: NT
ISAPI_Header	The header used when ISAPI_Mode is "HEADER", for example, blank.
ClaimType	Enter the SSO Claim Type. Default: **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn**

Stage 2 Execute configuration scripts

1. Open a PowerShell prompt.

   Note: If your server has User Account Control enabled, you must open the PowerShell prompt using elevated administrator permissions.

2. Navigate to the CP web service configuration directory, default:

   <cp_common>ConfigurationCPWebService

3. Execute: ./Configuration_SSO_ISAPI.ps1

4. Follow the prompts.

Configuring SSO using WS-Federation (ADFS 2.0) for WCF Web Services
Stage 1 Collect configuration parameters
Determine the values for the configuration parameters in the table, below. Ensure that the ADFS_Server_URI is in the Intranet zone of the end-user's browser.
Note: By default, Changepoint is configured to automatically update the public keys that are used to sign security tokens by using the published federation metadata document. In ADFS this is:
https://ADFS_Federation.ServiceName/FederationMetadata/2007-06/FederationMetadata.xml
In some cases it may not be possible to reach the ADFS server from the Changepoint web server so you will have to manually update the configuration after running the configuration script. For details, see "Manually updating public keys" on page 12.

Parameter	Description
WebService_Path	Location of the Changepoint WCF Web Services web application files. Default : <cp_root>\API\CP Web Services
WebService_URI	Domain identifier that you use for Changepoint WCF Web Services. For exam ple., **https://changepointapi.abc.corp/CPWebService**
Changepoint_RSA_ Cookie_Transform	Name of the certificate that you use for Cookie encryption. Default: the "CN=ChangepointApiCertificate" Certificate Name.
ServiceCertificate_Name	Certificate name that will be used to authenticate the service to clients using Message security mode. Default: the "CN=ChangepointApiCertificate" Certificate Name.
SigningCertificate_Name	Name of the certificate that you use for signing messages. Default: the "CN=ChangepointApiCertificate" Certificate Name is used.
ADFS_ FederationServiceName	Federation Service Name. To get the name: From the ADFS server, Launch ADFS 2.0 Management console. •Select ADFS 2.0 from the left menu. •From the Action pane select Edit Federation Service Properties. The Federation Service Name is on the General tab.
ClaimType	SSO Claim Type. The default is: **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn**

Stage 2 Execute configuration scripts
Configure the websites using the values for the configuration parameters.

1. Open a PowerShell prompt.

    Note: If your server has User Account Control enabled, you must open the PowerShell prompt using elevated

    administrator permissions.

2. Navigate to the Changepoint web service configuration directory, default:

    <cp_common>ConfigurationCPWebService

3.   Execute: ./Configuration_SSO_ADFS.ps1

4. Follow the prompts.

Stage 3 Create relying party trust
Create the Relying Party Trust in ADFS 2.0 Console.

1. On your ADFS server, launch the ADFS 2.0 console.

2. Select Action > Add Relying Party Trust.

3. Click Start.

4. Select Import data about the relying party published online or on a local network.

5. Enter the Federation metadata address, and then click Next, for example:

    https://changepointapi.abc.corp/cpwebservice/federationmetadata/2007-06/federationmetadata.xml

6. Enter a Display name, e.g. Changepoint WCF API, and click Next, Next, Next, then Close.

7. Add a Claim Rule for the above Changepoint Relying Party. For Changepoint, the default Claim rule name is

    "UPN".

8. Map the LDAP Attribute "User-Principal-Name" to Outgoing Claim Type "* UPN" or "UPN".

Manually updating public keys
To obtain the ADFS Server Token Signing Thumbprint

1. From the ADFS server, Launch ADFS 2.0 Management console.
2. Select Service > Certificates, and double-click the Token-signing certificate.
3. Select the Details tab.
4. Select the Thumbprint field.
5. To get the thumbprint value, remove all the spaces including the first space.

To update the Web.config file

1. Edit the ADFS web.config. The default location is:
   <cp_root>EnterpriseRP-STS_ADFS
2. Under the <appSettings> element, find the ida:FederationMetadataLocation key and clear its value:
   <add key="ida:FederationMetadataLocation" value="" />
3. Under <system.identityModel><identityConfiguration>, find the <issuerNameRegistry> element and replace it with the following: <issuerNameRegistry type="System.IdentityModel.Tokens.ValidatingIssuerNameRegistry, System.IdentityModel.Tokens.ValidatingIssuerNameRegistry"> <authority name="**https://ADFS_Federation.ServiceName/adfs/services/trust**"> <keys><add thumbprint="ADFS_Server_Token_Signing_Thumbprint"/></keys> <validIssuers> <add name="**https://ADFS_Federation.ServiceName/adfs/services/trust**" /> </validIssuers> </authority> </issuerNameRegistry>

Testing the COM API connection

1. Run the API Test Kit. The default location is:
   <cp_root>APIAPI ComponentsApiTestKit.exe.
2. Click Connection String > Encrypter.
3. In the Plain Text Connections String field:
   a. Replace SERVERNAME and DATABASENAME with your database information.
   b. Replace USERID and PASSWORD with your database admin user account information.
   c. Enter the timeout value as needed.
4. Click Encrypt.
5. In the Encrypted Connection String field, copy the text.
6. Close the dialog box.
7. On the API Test Kit menu, click Connection > COM API Connection Tester.
8. In the Current Version tab, paste the encrypted connection string into the Connection String field.
9. In the LoginId and Password fields, enter the login ID and password for your Changepoint account.
10. In the Loglevel (0-8) field, specify the level of error information to be returned in the COM API log file if the test result shows a problem with the connection.
    0 = No logging
    1 = Source object and method
    2 = Error message
    3 = Input parameters

4 = Returns

5 = Warning

8 = Checkpoint

The default is 8.

11. Click Connect.

If the connection was successful, a success message is displayed in the Result field. If the connection failed, check the COM API log file for errors. The default location of the log file is <cp_root>APIAPILogs.

Checking the version of installed API components

You can use the version checker utility to obtain details about the installed components, including the release version and path.

1. Run CPVersionChecker.exe. The default path is: <cp_root>APIAPI Components

2. Click Read.

Checking the version of the Web Services API

1. Launch Internet Explorer from the server where the Web Services API is installed, and enter the address: **http://localhost.port/CPWeb.Service/WSLogin.asmx** where port is the port number of the website where you installed the CPWebService virtual directory.

2. On the WSLogin page, click the GetVersion link.

3. Click Invoke.

Testing the Web Services API connection

1. Launch Internet Explorer from the server where the Web Services API is installed, and enter the address: **http://localhost.port/CPWeb.Service/WSLogin.asmx** where port is the port number of the website where you installed the CPWebService virtual directory.

2. On the WSLogin page click the TestConnection link.

3. Click Invoke. 4. In the test results:

- If <WSException> <HaveErrors> element is false, the test connection succeeded.
- If <WSException> <HaveErrors> element is true, the test connection failed. For more information on the reasons for the failure, see the <WSException> and <value> elements in the test results, and check the API logs. The default path to the API logs is: <cp_root>APIAPILogs

Setting up the Web Services API on a language server

1. To deploy the Changepoint Web Services API on a language server, you must add or update the <globalization> tag in the Web Services API web.config. The default location of the Web.config file is: <cp_root>APICP Web **ServicesWeb.config**

2. If the <globalization> tag already exists, ensure that both culture and uiCulture attributes are "en-US."

3. If the <globalization> tag does not already exist, add the following <globalization>, comment, and <compilation> elements to the <system.web> node: <system.web> <globalization culture="en-US" uiCulture="en-US" /> <!-Set compilation debug="true" to insert debugging symbols into the compiled page.

Because this affects performance, set this value to true only during development.

Visual Basic options: Set strict=" true" to disallow all data type conversions where data loss can occur. Set explicit="true" to force declaration of all variables. –> <compilation debug="true" strict="false" explicit="true">

4. Restart IIS.

Documents / Resources

API Installation Guide Reference Guide Changepoint 2021	**Changepoint API Software** [pdf] Installation Guide API, Software, API Software