Informatica® Managed File Transfer
10.5.0

REST API Guide

Informatica Managed File Transfer REST API Guide
10.5.0
August 2021

Publication Date: 2021-08-31

Table of Contents

Preface

Use the *REST API Guide* to learn how to call and run Informatica Managed File Transfer using the REST API. Learn how to design and implement transformations in Informatica Managed File Transfer file transfer entities. You can also learn how to perform administrative functions in Informatica Managed File Transfer using General, Project, Resource, and Web User REST APIs.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

REST API

This chapter includes the following topics:

REST API Overview

Informatica Managed File Transfer provides REST APIs that you can use to query and extract information regarding projects, connections, certificates, resources, web users, and job logs.

With Managed File Transfer REST APIs, you mitigate the necessity to perform all administrative activities through the Managed File Transfer console. Developers and administrators can use the REST APIs to automate activities and integrate Managed File Transfer administrative tasks with other tools.

Prerequisites

Before you can use REST APIs, create an admin user in Informatica Managed File Transfer.

Use the admin user credentials to perform the REST API calls.

CHAPTER 2

General APIs

This chapter includes the following topics:

General REST APIs Overview

You can use REST APIs to perform administrative functions in Informatica Managed File Transfer.

You can use the Ping MFT REST API to determine if Managed File Transfer is running. Use the Certificate Details REST API to obtain lists of certificates, private key aliases, and SSH keys.

You can use the Login Methods REST API to obtain a list of login methods. Use the Find SSH Key REST API to find an SSH key according to the identification number. Use the Job Log REST API to find an MFT job log according to the job log identification number.

Note: The response mime-type will be text or xml. Exception responses are in JSON format.

Ping Managed File Transfer REST API

Use the Ping Managed File Transfer REST API to check that Informatica Managed File Transfer is up and running. This API uses the GET method.

Use the following URL for the REST API call:

```
GET http://<hostName>:<portNumber>/informaticamft/api/v1/ping/dx
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

The following table describes the response body objects:

Object	Arguments
name	Name of the service that checks the status of Informatica Managed File Transfer.
status	The status of the service.

Response Body Example

The following code contains the response body syntax:

```
{ "name": "dx", "status": "success" }
```

Certificate Details REST API

Use the Certificate Details REST API to obtain the following Informatica Managed File Transfer information:

- list of certificates
- list of private key aliases available in the private keys key store
- list of all trusted certificate aliases available in the trusted-certificates key store
- list of all SSH private keys available in the SSH key manager
- list of SSH keys with RSA or DSA encryption

This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/certificates/search
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

To receive a list of certificates, include a request body. To specify which type of list you want to receive, provide a request body in JSON to the REST API call. The following table describes the request body objects:

Object	Arguments
keyStoreType	The type of keystore to search. The following options apply: - `X509PRIVATEKEY`: List of private key aliases available in the private keys key store. - `X509CERTIFICATE`: List of all trusted certificate aliases available in the trusted-certificates key store. - `SSH_PRIVATE_KEY`: List of SSH private keys.
algorithm	The type of information to search for. The following options apply: - `A`: List of all SSH private keys available in the SSH key manager - `R`: List of SSH keys with RSA encryption - `D`: List of SSH keys with DSA encryption

The following table describes the response body objects:

Object	Arguments
id	The identifying number of the certificate or key.
name	The name of the certificate or key.
privateKey	Identifies if the object is a private key.
size	The size of the certificate or key.
type	Identifies the type of object.
alias	The alias of the certificate or key.
subject	The subject of the certificate or key.
issuer	The issuer of the certificate or key.
fingerprint	The fingerprint of the certificate or key.

Request Body Examples

The following code shows the request body syntax to obtain a list of private key aliases available in the private keys key store:

```
{
   "keyStoreType":"X509PRIVATEKEY"
}
```

The following code shows the request body syntax to obtain a list of all trusted certificate aliases available in the trusted-certificates key store:

```
{
   "keyStoreType":"X509CERTIFICATE"
}
```

The following code shows the request body syntax to obtain a list of all SSH private keys available in the SSH key manager:

```
{
   "keyStoreType":"SSH_PRIVATE_KEY",
   "algorithm":"A"
}
```

The following code shows the request body syntax to obtain a list of SSH keys with RSA or DSA encryption:

```
{
   "keyStoreType":"SSH_PRIVATE_KEY",
   "algorithm":"R"
}
```

Response Body Examples

The following code shows the response body syntax with a list of all SSH private keys available in the SSH key manager:

```
[
   {
      "id":1011,
      "name":"sshkey",
      "privateKey":false,
      "algorithm":"R",
      "size":1024,
```

```
        "fingerprint":"28:04:E7:76:05:EA:64:CD:F3:88:E3:35:04:A2:21:AF"
    },
    {
        "id":1013,
        "name":"DSAKey",
        "privateKey":false,
        "algorithm":"D",
        "size":1024,
        "fingerprint":"4A:B6:03:23:88:BD:AC:82:52:8F:B3:D2:10:82:31:CC"
    }
]
```

The following code shows the response body syntax with a list of SSH keys with RSA or DSA encryption:

```
[
    {
        "id":1011,
        "name":"sshkey",
        "privateKey":false,
        "algorithm":"R",
        "size":1024,
        "fingerprint":"28:04:E7:76:05:EA:64:CD:F3:88:E3:35:04:A2:21:AF"
    }
]
```

Login Methods REST API

Use the Login Methods REST API to obtain a list of Informatica Managed File Transfer login methods. This API uses the GET method.

Use the following URL for the REST API call:

```
GET http://<hostName>:<portNumber>/informaticamft/api/v1/webusers/loginmethods
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON to the REST API call. The following table describes the request body objects:

The following table describes the response body objects:

Object	Arguments
id	Specify the login method identification number.
name	User name of the login method.

Response Body Examples

The following code shows a response body:

```
{
        "id":1001,
        "name":"Infa"
    },
    {
        "id":1002,
        "name":"Infa-ISP"
    },
```

```
{
   "id":1003,
   "name":"Infa-LDAPS"
},
{
   "id":101,
   "name":"Native"
}
```

Find SSH Key REST API

Use the Find SSH Key REST API to find an Informatica Managed File Transfer SSH Key according to an identification number. This API uses the GET method.

Use the following URL for the REST API call:

```
GET http://<hostName>:<portNumber>/informaticamft/api/v1/sshkeys/{id}
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

The following table describes the variable:

Object	Arguments
id	Specify the SSH Key database identification number.

The following table describes the response body objects:

Object	Arguments
id	The identifying number of the key.
name	The name of the key.
privateKey	Identifies if the object is a private key.
algorithm	Identifies the encryption algorithm.
size	The size of the key.
fingerprint	The fingerprint of the key.
comments	Comment describing the key.
privateKeyPassword	The password for the key.
createdBy	Identifies the creator of the key.
keyBytes	The actual bytes that the key consists of.

Response Body Examples

The following code shows a response body:

```
{
   "id":1011,
   "name":"sshkey",
   "privateKey":true,
   "algorithm":"R",
   "size":1024,
   "fingerprint":"28:04:E7:76:05:EA:64:CD:F3:88:E3:35:04:A2:21:AF",
   "comments":"",
   "privateKeyPassword":"Admin@123",
   "createdBy":"sys",
   "createdOn":1487593778633,
   "keyBytes":"LS0tLS1CRUdJTiBZBVEUgS0VZLS0tLS0NCg=="
}
```

Job Log REST API

Use the Job Log REST API to find an Informatica Managed File Transfer job log according to the job identification number. This API uses the GET method.

Use the following URL for the REST API call:

```
GET http://<hostName>:<portNumber>/informaticamft/api/v1/job/{jobId}
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

The following table describes the call variable:

Object	Arguments
jobId	Specify the MFT job log identification number.

Response Body Examples

The following code shows a response body:

```
[
   "4/3/17 12:55:00 PM INFO Start Date and Time: 4/3/17 12:55:00 PM",
   "4/3/17 12:55:00 PM INFO Job Number: 1000000000391 ",
   "4/3/17 12:55:00 PM INFO Project Name: /FTPReceive",
   "4/3/17 12:55:00 PM INFO Submitted By: administrator",
   "4/3/17 12:55:00 PM INFO Submitted From: REST API",
   "4/3/17 12:55:00 PM INFO Informatica Managed File Transfer 10.2.0 running on Windows
10 10.0 (amd64)",
   "4/3/17 12:55:00 PM INFO Overriding variable 'DX_EndpointName' with value 'RR'",
   "4/3/17 12:55:00 PM INFO Overriding variable 'DX_FileDownloadDir' with value 'c:/Temp\
\RR'",
   "4/3/17 12:55:00 PM INFO Overriding variable 'DX_Partner' with value 'P1'",
   "4/3/17 12:55:00 PM INFO Overriding variable 'DX_Account' with value 'A1'",
   "4/3/17 12:55:00 PM INFO Executing project 'FTPReceive' ",
   "4/3/17 12:55:00 PM INFO Project location: C:\\Informatica\\B2B\\MFT\\server\\userdata
\\projects\\FTPReceive.xml",
   "4/3/17 12:55:00 PM INFO Executing module 'Main'",
   "4/3/17 12:55:00 PM INFO Executing task 'ftp 1.0'",
   "4/3/17 12:55:00 PM INFO Connecting to 'localhost' at port '21' as user 'Test' ",
   "4/3/17 12:55:00 PM INFO Executing sub-task 'get'",
```

```
   "4/3/17 12:55:00 PM INFO Setting the data type to AUTO",
   "4/3/17 12:55:00 PM INFO Downloading '/Out/1046.out' to 'C:\\FlatFile\\Input\\test\
\1046.out'",
   "4/3/17 12:55:01 PM INFO File '/Out/1046.out' successfully downloaded to 'C:\\FlatFile
\\Input\\test\\1046.out' (86 bytes)",
   "4/3/17 12:55:01 PM INFO 1 file(s) were downloaded successfully ",
   "4/3/17 12:55:01 PM INFO Finished sub-task 'get'",
   "4/3/17 12:55:01 PM INFO Closed the FTP connection",
   "4/3/17 12:55:01 PM INFO Finished task 'ftp 1.0'",
   "4/3/17 12:55:01 PM INFO Executing task 'rename 1.0'",
   "4/3/17 12:55:01 PM INFO File 'C:\\FlatFile\\Input\\test\\1046.out' was successfully
renamed to 'C:\\FlatFile\\Input\\test\\a.in' (86 bytes)",
   "4/3/17 12:55:01 PM INFO 1 file(s) were renamed successfully",
   "4/3/17 12:55:01 PM INFO Finished task 'rename 1.0'",
   "4/3/17 12:55:01 PM INFO Finished module 'Main'",
   "4/3/17 12:55:01 PM INFO Finished project 'FTPReceive'",
   "4/3/17 12:55:01 PM INFO End Date and Time: 4/3/17 12:55:01 PM"
]
```

Password Encryption REST API

Use the Encrypt Password REST API to encrypt a phrase that can then be used in a variable to pass to a *Project*. This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/encryptPassword
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON to the REST API call. The following table describes the request body object:

Object	Arguments
password	Enter the text that should be encrypted.

Request Body Example

The following code shows the request body syntax:

```
{
"password": "Hello"
  }
```

Response Body Example

The following code shows a response:

```
"3yN10Ct4LQs="
```

CHAPTER 3

Project REST APIs

This chapter includes the following topics:

Project REST APIs Overview

Projects are used to describe the work for Managed File Transfer to perform. For instance, a Project definition can indicate where to retrieve data from, what file transfer tasks to perform (for example Zip or encrypt) and where to send the file.

Use the Project REST APIs to manage Managed File Transfer projects. You can obtain a list of projects, the definitions and variable settings for a project, or the timestamp for the last project modification.

Project List REST API

Use the Project List REST API to obtain a list of Informatica Managed File Transfer projects sorted according to path, folder, and project ID categories. This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/projects/search
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON to the REST API call. The following table describes the request body objects:

Object	Arguments
categoryId	Obtain a list of projects identified by ID.
path	Obtain a list of projects identified by the path at which the project file is located.
category	Obtain a list of projects identified by the name of the directory in which the project file is located or the name of the project file.

The following table describes the response body objects:

Object	Arguments
id	The identifying number of the project.
name	Name of the project.
description	Description of the project.
path	Path at which the project file is located, or list of projects according to path.
folders	List of projects according to directory in which the project is located.
projects	List of projects.

Request Body Example

The following code shows the request body syntax:

```
{
 "categoryId": "102",
 "path": "/DXProjects"
}
```

Response Body Example

The following code shows the response body syntax:

```
{
   "path":"/DXProjects",
   "folders":[
      {
         "id":1001,
         "name":"DataExchange",
         "path":"/DataExchange"
      },
      {
         "id":102,
         "name":"DXProjects",
         "description":"DX Projects",
         "path":"/DXProjects"
      }
   ],
   "projects":[
      {
         "id":1055,
         "name":"Cha",
         "path":"/Cha"
      },
```

```
      {
         "id":1056,
         "name":"ChangeDir",
         "path":"/ChangeDir"
      }
   ]
}
```

Project Definition REST API

Use the Project Definition REST API to obtain full details for a Informatica Managed File Transfer project. This API uses the GET method.

Use the following URL for the REST API call:

```
GET http://<hostName>:<portNumber>/informaticamft/api/v1/projectsxml/{Project}
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

In this URL, `{Project}` represents the variable `Project` set to the path for the project, for example:

```
Project = "DXProjects/Receive/DX_Remote_FTPS_Receive"
```

The resulting project XML file is delivered to the `<MFT Installation>\userdata\projects` directory.

You can also view the project XML file location in the Informatica File Transfer Portal. Select **System** > **Global Settings** > **Data** > **Projects Directory**.

XML Output Example

The following code shows the XML output syntax:

```
<?xml version="1.0" encoding="UTF-8" ?>
<projectname="DX_Remote_FTPS_Receive"mainModule="Main"version="2.0"logLevel="verbose"thre
adSafe="true">
<modulename="Main"onError="call:ErrorModule">
<iflabel="if RegEx"condition="${Upper(RegEx_or_WildCard)==Upper(&apos;Regex&apos;)}">
<else>
<iflabel="if WildCard"condition="${Upper(RegEx_or_WildCard)==
Upper(&apos;Wildcard&apos;)}">…</if>
</else>
<ftpslabel="Connect to FTPS server"resourceId="$
{Source_FTPS_Connection}"outputSessionId="${FTPSSession}"version="1.0">
<getdestinationDir="$
{DX_FileDownloadDir}"whenFileExists="rename"processedSourceFilesVariable="$
{remoteFileList}">…</get>
</ftps>
<iflabel="Delete_From_Source_After_Download"condition="$
{Delete_From_Source_After_Download==&apos;true&apos;}">
<ftpslabel="Connect to FTPS server"resourceId="$
{Source_FTPS_Connection}"inputSessionId="${FTPSSession}"version="1.0">…</ftps>
</if>
</if>
</module>
<description>A Project for receiving files from a remote FTPS resource. Uses variables
for seamless integration with B2B DX.</description>
<variablename="Source_FTPS_Connection"value="""description="Select a pre-configured
FTPS server connection. This variable is mandatory."/>
<variablename="Source_Directory"value="/"description="Specify a directory from which
files will be downloaded."/>
<variablename="RegEx_or_WildCard"value="WildCard"description="Specify whether to use a
Wild Card Filter or a Regular Expression Filter to search for file(s) to download.
```

```
Accepted values: WildCard or RegEx."/>
<variablename="File_Pattern_To_Download"value="*.in"description="Specify the file name
pattern for download."/>
<variablename="Delete_From_Source_After_Download"value="true"description="Specify
whether to delete to the file from source after download. Accepted values: true or
false."/>
<variablename="SMTP_Server"value=""""description="Specify the SMTP server to be used to
sending error notification. This variable is optional."/>
<variablename="Email_For_Notification"value=""""description="Specify the email address
of the user to be notified in case the MFT project fails."/>
<modulename="ErrorModule"onError="continue">
<iflabel="Check for SMTP server value"condition="${IsNotEmpty(SMTP_Server)}">
<sendEmaillabel="Send Error email"resourceId="${SMTP_Server}"toList="$
{Email_For_Notification}"version="2.0">
<fromaddress="admin@infamft.com"/>
<subject><![CDATA[Project ${system.project.name} Failed]]></subject>
<messagefile="${system.job.log}"><![CDATA[Project ${system.project.name} failed due to
the following reason: ${system.job.error}]]></message>
</sendEmail>
</if>
<raiseErrorversion="1.0">
<message>
Project ${system.project.name} failed due to the following reason:
${system.job.error}
</message>
</raiseError>
</module>
</project>
```

Project Modification Timestamp REST API

Use the Project Modification Timestampe REST API to obtain the date and time that a Informatica Managed File Transfer project was modified. This API uses the GET method.

Use the following URL for the REST API call:

```
GET http://<hostName>:<portNumber>/informaticamft/api//v1/projects/{Project}
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

In this URL, `{Project}` represents the variable `Project` set to the path for the project, for example:

```
Project = "DXProjects/Receive/DX_Remote_FTPS_Receive"
```

The following table describes the response body objects:

Object	Arguments
modifiedDate	The timestamp of the last time that the project was modified.

Response Body Example

The following code shows the response body syntax:

```
{
"modifiedDate": "15-02-2017 11:12:03"
}
```

CHAPTER 4

Resource REST APIs

This chapter includes the following topics:

Resource REST API Overview

Resources are the names and connection properties of the servers, and other data sources, that Managed File Transfer can interact with.

Use the Resource REST APIs to manage Managed File Transfer resources. You can obtain a list of resources, the number of resources currently defined, or create a resource. You can get the default settings for any type of resource.

You can update the resource definitions, or delete a resource. You can also test a resource connection.

Resource List REST API

Use the Resource List REST API to obtain a list of Informatica Managed File Transfer resources based on a search expression. This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/resources/search
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON to the REST API call. The following table describes the request body objects:

Object	Arguments
firstResult	Specify the first result to present.
maxResults	Specify the maximum number of results to present.
selectedSortColumn	Select which column is used to sort the resource information.
sortAscending	Sort the resources in ascending order.
matchAll	Provide all the matches to the search expression when performing the search.
useExactMatch	Exactly match the search expression when performing the search.
simpleSearchString	Use a simple search string to perform the search.
simpleSearch	Use a simple search to perform the search.
searchString	Specify the search string used to perform the search.
types	Select the resource type to search for. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox

The following table describes the response body objects:

Object	Arguments
id	Identifying number for the resource.
name	Name of the resource.
description	Description of the resource.
type	Type of resource, for example `ftp`.
modifiedDate	Date that the resource was last modified.

Request Body Example

The following code shows the request body syntax:

```
{
   "firstResult":0,
   "maxResults":50,
   "selectedSortColumn":1,
   "sortAscending":true,
   "matchAll":true,
```

```
    "useExactMatch":false,
    "simpleSearchString":null,
    "simpleSearch":false,
    "searchString":null,
    "types":[
       "ftp",
       "ftps",
       "ssh",
       "as2",
       "http",
       "https",
       "smtp",
       "mq",
       "mailbox"
    ]
}
```

Response Body Example

The following code shows the response body syntax:

```
[
   {
      "id":1043,
      "name":"ftpRes",
      "description":"descriptionFtp",
      "type":"ftp",
      "modifiedDate":1490863585583
   },
   {
      "id":1095,
      "name":"SmtpRes",
      "description":"descriptionSmtp",
      "type":"smtp",
      "modifiedDate":1486985704210
   },
   {
      "id":1094,
      "name":"SshRes",
      "description":"descriptionSsh",
      "type":"ssh",
      "modifiedDate":1486985572883
   }
]
```

Resource Count REST API

Use the Resource Count REST API to obtain the number of Informatica Managed File Transfer resources based on a search expression. This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/resources/count
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON to the REST API call. The following table describes the request body objects:

Object	Arguments
firstResult	Specify the first result to present.
maxResults	Specify the maximum number of results to present.
selectedSortColumn	Select which column is used to sort the resource information.
sortAscending	Sort the resources in ascending order.
matchAll	Provide all the matches to the search expression when performing the search.
useExactMatch	Exactly match the search expression when performing the search.
simpleSearchString	Use a simple search string to perform the search.
simpleSearch	Use a simple search to perform the search.
searchString	Specify the search string used to perform the search.
types	Select the resource type to search for. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox

Request Body Example

The following code shows the request body syntax:

```
{
   "firstResult":0,
   "maxResults":50,
   "selectedSortColumn":1,
   "sortAscending":true,
   "matchAll":true,
   "useExactMatch":false,
   "simpleSearchString":null,
   "simpleSearch":false,
   "searchString":null,
   "types":[
      "ftp",
      "ftps",
      "ssh",
      "as2",
      "http",
      "https",
      "smtp",
      "mq",
      "mailbox"
   ]
}
```

Response Body Example

The following code shows a response:

```
20
```

Create Resource REST API

Use the Create Resource REST API to create an Informatica Managed File Transfer resource. This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/resources
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON to the REST API call. The following table describes the request body objects:

Object	Arguments
id	Specify the resource identification number.
type	Select the type of resource to create. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox
name	Name of the resource.
description	Description of the resource.
resourceObject	Container element to encapsulate the resource properties.
resourceName	Name of the resource.
resourceDescription	Description of the resource.
primaryContactName	The name of the primary contact for the resource.
secondaryContactName	The name of the secondary contact for the resource.
primaryContactPhone	The phone number of the primary contact for the resource.
secondaryContactPhone	The phone number of the secondary contact for the resource.

Object	Arguments
primaryContactEmail	The email address of the primary contact for the resource.
secondaryContactEmail	The email address of the secondary contact for the resource.
host	The host name or IP address of the server.
port	The port number to use to connect to the server. If left blank, the default port number is 21.
user	The user name to use to connect to the server.
password	The password to use to connect to the server.
passwordIsEncrypted	Indicates whether or not the password is encrypted.
timeout	The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time.
connectionRetryAttempts	The number of times to retry the connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If
connectionRetryInterval	The number of seconds to wait between each connection retry attempt.
initialRemoteDirectory	The initial directory to start in after connecting to the server.
controlEncoding	If left blank, Managed File Transfer uses the ISO standard ISO-8859-1. If supported by the server, other encodings like UTF-8 can be specified to support more international characters.
throttleBandwidth	Limit the inbound and outbound bandwidth used for file transfers.
proxyType	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers may support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.
proxyHost	The host name or IP address of the proxy server.
alternateProxyHost	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
proxyPort	The port number to use for connecting to the proxy server.
proxyUser	The user name to use to connect to the proxy server.
proxyPassword	The password to use for connecting to the proxy server.
proxyPasswordIsEncrypted	Indicates whether or not the password is encrypted.
passive	Indicates whether or not the connection will use Passive or Active mode. Specify Yes to use Passive mode. Specify No to use Active mode.

Object	Arguments
listParser	The list parser to use for the server connection. If the field is left blank, Managed File Transfer will attempt to use the MLSD parser. If the MLSD parser is not supported by the server, the UNIX parser will be used.
dateFormat	This field is used if the date returned by the server is different than the selected list parser's default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the Date Format setting will ignore any User specified values.
recentDateFormat	Specify the date format to use when parsing the recent last modified date for each file. The recent date format is primarily used on UNIX-based systems and appears on entries less than a year old. If your location requires a different recent date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting will ignore any User specified values.
dataConnectionStartPort	The starting port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
dataConnectionEndPort	The ending port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
type	Select the type of resource to create. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox
resourceType	Select the type of resource to create. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox

Request Body Example

The following code shows the request body syntax:

```
{
   "id":-1,
   "type":"ftp",
   "name":"",
   "description":"",
   "resourceObject":{
      "resourceName":"test",
      "resourceDescription":"Description",
```

```
      "primaryContactName":null,
      "secondaryContactName":null,
      "primaryContactPhone":null,
      "secondaryContactPhone":null,
      "primaryContactEmail":null,
      "secondaryContactEmail":null,
      "host":"localhost",
      "port":"21",
      "user":"Admin",
      "password":"Admij",
      "passwordIsEncrypted":null,
      "timeout":"20",
      "connectionRetryAttempts":"4",
      "connectionRetryInterval":"6",
      "initialRemoteDirectory":"C:/FTP",
      "controlEncoding":null,
      "throttleBandwidth":"true",
      "proxyType":"http",
      "proxyHost":"localhost",
      "alternateProxyHost":"altHost",
      "proxyPort":"15021",
      "proxyUser":"Admin",
      "proxyPassword":"Admin",
      "proxyPasswordIsEncrypted":null,
      "passive":"true",
      "listParser":"unix",
      "dateFormat":null,
      "recentDateFormat":null,
      "dataConnectionStartPort":"10000",
      "dataConnectionEndPort":"20000",
      "type":"ftp",
      "resourceType":"ftp"
   },
   "createdBy":null,
   "createdOn":null,
   "modifiedBy":null,
   "modifiedOn":null
}
```


Response Body Example

The following code shows a response:


```
{
   "id":1348,
   "type":"ftp",
   "name":"test",
   "description":"Description",
   "resourceObject":{
      "resourceName":"test2",
      "resourceDescription":"Description",
      "host":"localhost",
      "port":"21",
      "user":"Admin",
      "password":"lfyYJvYxNmQ=",
      "passwordIsEncrypted":"true",
      "timeout":"20",
      "connectionRetryAttempts":"4",
      "connectionRetryInterval":"6",
      "initialRemoteDirectory":"C:/FTP",
      "throttleBandwidth":"true",
      "proxyType":"http",
      "proxyHost":"localhost",
      "alternateProxyHost":"altHost",
      "proxyPort":"15021",
      "proxyUser":"Admin",
      "proxyPassword":"KwCSbW/Go+Y=",
      "proxyPasswordIsEncrypted":"true",
      "passive":"true",
      "listParser":"unix",
      "dataConnectionStartPort":"10000",
```

```
        "dataConnectionEndPort":"20000",
        "type":"ftp",
        "resourceType":"ftp"
    },
    "createdBy":"sys",
    "javascriptEscapedName":"test"
}
```

Delete Resource REST API

Use the Delete Resource Definition REST API to delete a Informatica Managed File Transfer resource according to the resource ID. This API uses the DELETE method.

Use the following URL for the REST API call:

```
DELETE http://<hostName>:<portNumber>/informaticamft/api/v1/resources/{resourceId}
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

The following table describes the request variable:

Object	Arguments
resourceId	The database identification number for the resource. **Note:** When a resource is created, the database identification number (databaseId) is provided in resource object.

The following table describes the response body objects:

Object	Arguments
1	The resource was successfully deleted.
responseCode	If unsuccessful, the API returns the response code `RESOURCE_NOT_FOUND`..
message	If unsuccessful, the API returns a descriptive message.

Response Body Example

The following code shows a response:

```
{ 1
}
```

Update Resource REST API

Use the Update Resource REST API to update an Informatica Managed File Transfer resource that you identify according to resource ID. This API uses the PUT method.

Use the following URL for the REST API call:

```
PUT http://<hostName>:<portNumber>/informaticamft/api/v1/resources/{resourceId}
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

The following table describes the request variable:

Object	Arguments
resourceId	The database identification number for the resource.

You can provide a request body in JSON to the REST API call. The following table describes the request body objects:

Object	Arguments
id	Specify the resource identification number.
type	Select the type of resource to create. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox
name	Name of the resource.
description	Description of the resource
resourceObject	Container element to encapsulate the resource properties.
resourceName	Name of the resource.
resourceDescription	Description of the resource.
primaryContactName	The name of the primary contact for the resource.
secondaryContactName	The name of the secondary contact for the resource.
primaryContactPhone	The phone number of the primary contact for the resource.
secondaryContactPhone	The phone number of the secondary contact for the resource.

Object	Arguments
primaryContactEmail	The email address of the primary contact for the resource.
secondaryContactEmail	The email address of the secondary contact for the resource.
host	The host name or IP address of the server.
port	The port number to use to connect to the server. If left blank, the default port number is 21.
user	The user name to use to connect to the server.
password	The password to use to connect to the server.
passwordIsEncrypted	Indicates whether or not the password is encrypted.
timeout	The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time.
connectionRetryAttempts	The number of times to retry the connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If
connectionRetryInterval	The number of seconds to wait between each connection retry attempt.
initialRemoteDirectory	The initial directory to start in after connecting to the server.
controlEncoding	If left blank, Managed File Transfer uses the ISO standard ISO-8859-1. If supported by the server, other encodings like UTF-8 can be specified to support more international characters.
throttleBandwidth	Limit the inbound and outbound bandwidth used for file transfers.
proxyType	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers may support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.
proxyHost	The host name or IP address of the proxy server.
alternateProxyHost	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
proxyPort	The port number to use for connecting to the proxy server.
proxyUser	The user name to use to connect to the proxy server.
proxyPassword	The password to use for connecting to the proxy server.
proxyPasswordIsEncrypted	Indicates whether or not the password is encrypted.
passive	Indicates whether or not the connection will use Passive or Active mode. Specify Yes to use Passive mode. Specify No to use Active mode.

Object	Arguments
listParser	The list parser to use for the server connection. If the field is left blank, Managed File Transfer will attempt to use the MLSD parser. If the MLSD parser is not supported by the server, the UNIX parser will be used.
dateFormat	This field is used if the date returned by the server is different than the selected list parser's default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the Date Format setting will ignore any User specified values.
recentDateFormat	Specify the date format to use when parsing the recent last modified date for each file. The recent date format is primarily used on UNIX-based systems and appears on entries less than a year old. If your location requires a different recent date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting will ignore any User specified values.
dataConnectionStartPort	The starting port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
dataConnectionEndPort	The ending port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
type	Select the type of resource to create. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox
resourceType	Select the type of resource to create. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox
createdBy	Specify the entity that created the resource.
createdOn	Specify when the resource was created.
modifiedBy	Specify the entity that modified the resource.
modifiedOn	Specify when the resource was modified.

Request Body Example

The following code shows the request body syntax:


```
{
   "id":1346,
   "type":"ftp",
   "name":"test",
   "description":"Description",
   "resourceObject":{
      "resourceName":"test",
      "resourceDescription":"Description",
      "host":"localhost",
      "port":"21",
      "user":"Admin",
      "passwordIsEncrypted":"true",
      "timeout":"20",
      "connectionRetryAttempts":"4",
      "connectionRetryInterval":"6",
      "initialRemoteDirectory":"C:/FTP",
      "throttleBandwidth":"true",
      "proxyType":"http",
      "proxyHost":"localhost",
      "alternateProxyHost":"altHost",
      "proxyPort":"15021",
      "proxyUser":"Admin",
      "proxyPasswordIsEncrypted":"true",
      "passive":"true",
      "listParser":"unix",
      "dataConnectionStartPort":"10000",
      "dataConnectionEndPort":"20000",
      "type":"ftp",
      "resourceType":"ftp"
   },
   "createdBy":"sys",
   "createdOn":1491053640230,
   "modifiedBy":"sys",
   "modifiedOn":1491135776623,
   "javascriptEscapedName":"test"
}
```


Response Body Example

The following code shows a response:


```
{
   "id":1346,
   "type":"ftp",
   "name":"test",
   "description":"Description",
   "resourceObject":{
      "resourceName":"test",
      "resourceDescription":"Description",
      "host":"localhost",
      "port":"21",
      "user":"Admin",
      "password":"lfyYJvYxNmQ=",
      "passwordIsEncrypted":"true",
      "timeout":"20",
      "connectionRetryAttempts":"4",
      "connectionRetryInterval":"6",
      "initialRemoteDirectory":"C:/FTP",
      "throttleBandwidth":"true",
      "proxyType":"http",
      "proxyHost":"localhost",
      "alternateProxyHost":"altHost",
      "proxyPort":"15021",
      "proxyUser":"Admin",
      "proxyPassword":"KwCSbW/Go+Y=",
      "proxyPasswordIsEncrypted":"true",
      "passive":"true",
```

```
        "listParser":"unix",
        "dataConnectionStartPort":"10000",
        "dataConnectionEndPort":"20000",
        "type":"ftp",
        "resourceType":"ftp"
    },
    "createdBy":"sys",
    "createdOn":1491053640230,
    "modifiedBy":"sys",
    "modifiedOn":1491135776623,
    "javascriptEscapedName":"test"
}
```


Test Resource Connection REST API

Use the Test Resource Connection REST API to test the connection for an Informatica Managed File Transfer resource. This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/resource/test
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON to the REST API call. The following table describes the request body objects:

Object	Arguments
id	Specify the resource identification number.
type	Select the type of resource. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox
name	Name of the resource.
description	Description of the resource.
resourceObject	Container element to encapsulate the resource properties.
resourceName	Name of the resource.
resourceDescription	Description of the resource.
primaryContactName	The name of the primary contact for the resource.

Object	Arguments
secondaryContactName	The name of the secondary contact for the resource.
primaryContactPhone	The phone number of the primary contact for the resource.
secondaryContactPhone	The phone number of the secondary contact for the resource.
primaryContactEmail	The email address of the primary contact for the resource.
secondaryContactEmail	The email address of the secondary contact for the resource.
host	The host name or IP address of the server.
port	The port number to use to connect to the server. If left blank, the default port number is 21.
user	The user name to use to connect to the server.
password	The password to use to connect to the server.
passwordIsEncrypted	Indicates whether or not the password is encrypted.
timeout	The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time.
connectionRetryAttempts	The number of times to retry the connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If
connectionRetryInterval	The number of seconds to wait between each connection retry attempt.
initialRemoteDirectory	The initial directory to start in after connecting to the server.
controlEncoding	If left blank, Managed File Transfer uses the ISO standard ISO-8859-1. If supported by the server, other encodings like UTF-8 can be specified to support more international characters.
throttleBandwidth	Limit the inbound and outbound bandwidth used for file transfers.
proxyType	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers may support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.
proxyHost	The host name or IP address of the proxy server.
alternateProxyHost	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
proxyPort	The port number to use for connecting to the proxy server.
proxyUser	The user name to use to connect to the proxy server.

Object	Arguments
proxyPassword	The password to use for connecting to the proxy server.
proxyPasswordIsEncrypted	Indicates whether or not the password is encrypted.
passive	Indicates whether or not the connection will use Passive or Active mode. Specify Yes to use Passive mode. Specify No to use Active mode.
listParser	The list parser to use for the server connection. If the field is left blank, Managed File Transfer will attempt to use the MLSD parser. If the MLSD parser is not supported by the server, the UNIX parser will be used.
dateFormat	This field is used if the date returned by the server is different than the selected list parser's default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the Date Format setting will ignore any User specified values.
recentDateFormat	Specify the date format to use when parsing the recent last modified date for each file. The recent date format is primarily used on UNIX-based systems and appears on entries less than a year old. If your location requires a different recent date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting will ignore any User specified values.
dataConnectionStartPort	The starting port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
dataConnectionEndPort	The ending port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
type	Select the type of resource to create. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox
resourceType	Select the type of resource to create. The following options apply: - ftp - ftps - ssh - as2 - http - https - smtp - mq - mailbox
createdBy	Specify the entity that created the resource.

Object	Arguments
createdOn	Specify when the resource was created.
modifiedBy	Specify the entity that modified the resource.
modifiedOn	Specify when the resource was modified.

Request Body Example

The following code shows the request body syntax:

```
{
   "id":1133,
   "type":"ftp",
   "name":"TLVXE4",
   "description":null,
   "resourceObject":{
      "resourceName":"TLVXE4",
      "resourceDescription":null,
      "primaryContactName":null,
      "secondaryContactName":null,
      "primaryContactPhone":null,
      "secondaryContactPhone":null,
      "primaryContactEmail":null,
      "secondaryContactEmail":null,
      "host":"TLVXE4",
      "port":"21",
      "user":"infa",
      "password":null,
      "passwordIsEncrypted":null,
      "timeout":null,
      "connectionRetryAttempts":null,
      "connectionRetryInterval":null,
      "initialRemoteDirectory":null,
      "controlEncoding":null,
      "throttleBandwidth":null,
      "proxyType":null,
      "proxyHost":null,
      "alternateProxyHost":null,
      "proxyPort":null,
      "proxyUser":null,
      "proxyPassword":null,
      "proxyPasswordIsEncrypted":null,
      "passive":null,
      "listParser":null,
      "dateFormat":null,
      "recentDateFormat":null,
      "dataConnectionStartPort":null,
      "dataConnectionEndPort":null,
      "type":"ftp",
      "resourceType":"ftp"
   },
   "createdBy":"sys",
   "createdOn":1487136787107,
   "modifiedBy":"sys",
   "modifiedOn":1487136787107
}
```

Response Body Examples

The following code shows a response body for a successful test:

```
{
   "success":true,
   "messages":[
      {
```

```
            "timestamp":"04/92/17 06:24:58 PM",
            "messageType":"INFO",
            "message":"Connecting to 'TLVXE4'"
         },
         {
            "timestamp":"04/92/17 06:25:01 PM",
            "messageType":"INFO",
            "message":"Logging in to the server."
         },
         {
            "timestamp":"04/92/17 06:25:01 PM",
            "messageType":"INFO",
            "message":"Current working directory is '/users/infa'."
         },
         {
            "timestamp":"04/92/17 06:25:01 PM",
            "messageType":"INFO",
            "message":"Retrieving directory listing. "
         },
         {
            "timestamp":"04/92/17 06:25:03 PM",
            "messageType":"INFO",
            "message":"Listing raw files. (Up to 5 of 375)."
         },
         {
            "timestamp":"04/92/17 06:25:03 PM",
            "messageType":"INFO",
            "message":"-rw-r--r-- 1 2210 1021 3 Aug 19 2015 1000.out"
         },
         {
            "timestamp":"04/92/17 06:25:03 PM",
            "messageType":"INFO",
            "message":"-rw-r--r-- 1 2210 1021 3 Aug 19 2015 1001.out"
         },
         {
            "timestamp":"04/92/17 06:25:03 PM",
            "messageType":"INFO",
            "message":"-rwxrwxrwx 1 2210 1021 22 May 28 2014 1111.in.mi"
         },
         {
            "timestamp":"04/92/17 06:25:03 PM",
            "messageType":"INFO",
            "message":"-rw-r--r-- 1 2210 1021 40666 Mar 08 2016 1_130001.out"
         },
         {
            "timestamp":"04/92/17 06:25:03 PM",
            "messageType":"INFO",
            "message":"-rw-r--r-- 1 2210 1021 176 Nov 15 2015 229211.out"
         },
         {
            "timestamp":"04/92/17 06:25:03 PM",
            "messageType":"INFO",
            "message":"-rwxr-xr-x 1 2210 1021 329 Apr 25 2016
850_5030_Valid_1ST_1GS_1PO.bak"
         },
         {
            "timestamp":"04/92/17 06:25:05 PM",
            "messageType":"INFO",
            "message":"Listing parsed remote files. (Up to 5 of 374)."
         },
         {
            "timestamp":"04/92/17 06:25:05 PM",
            "messageType":"INFO",
            "message":"1000.out (3, 8/19/15 12:00:00 AM)"
         },
         {
            "timestamp":"04/92/17 06:25:05 PM",
            "messageType":"INFO",
            "message":"1001.out (3, 8/19/15 12:00:00 AM)"
         },
         {
```

```
            "timestamp":"04/92/17 06:25:05 PM",
            "messageType":"INFO",
            "message":"1111.in.mi (22, 5/28/14 12:00:00 AM)"
         },
         {
            "timestamp":"04/92/17 06:25:05 PM",
            "messageType":"INFO",
            "message":"1_130001.out (40,666, 3/8/16 12:00:00 AM)"
         },
         {
            "timestamp":"04/92/17 06:25:05 PM",
            "messageType":"INFO",
            "message":"229211.out (176, 11/15/15 12:00:00 AM)"
         },
         {
            "timestamp":"04/92/17 06:25:06 PM",
            "messageType":"INFO",
            "message":"Disconnecting from server."
         }
      ]
   }
```

The following code shows a response body for a failed test:

```
   {
      "success":false,
      "messages":[
         {
            "timestamp":"04/92/17 06:27:44 PM",
            "messageType":"INFO",
            "message":"Connecting to 'TLVXE4'"
         },
         {
            "timestamp":"04/92/17 06:27:45 PM",
            "messageType":"ERROR",
            "message":"Could not parse response code.\nServer Reply: SSH-2.0-OpenSSH_5.3"
         },
         {
            "timestamp":"04/92/17 06:27:45 PM",
            "messageType":"INFO",
            "message":"Disconnecting from server."
         }
      ],
      "stackTrace":"com.linoma.ga.projects.tasks.ftp.FTPInterfaceException: Could not parse
   response code.
   \nCaused by: org.apache.commons.net.MalformedServerReplyException: Could not parse
   response code."
   }
```

CHAPTER 5

Web User REST APIs

This chapter includes the following topics:

Web User Rest API Overview

Use the Web User REST APIs to manage Managed File Transfer web users.

You can create a web user and apply a template, add the web user, and obtain the number of web users currently defined. You can find a web user using a search string, or according to an identification number.

Create Web User REST API

Use the **webusers** REST API to create and get an Informatica Managed File Transfer web user from a template. This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/webusers
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

The following table describes the request body objects:

Object	Arguments
id	Specify the web user identification number.
name	User name of the web user.
firstName	First name of the web user.
lastName	Last name of the web user.
description	Description of the web user.
password	The password associated with the web user.
passwordIsEncrypted	Indicates whether or not the password is encrypted.
passwordHashAlgorithm	Indicates whether or not the password is encrypted with a hash algorithm. The following hash algorithms are supported: - MD2 - MD5 - SHA-1 - SHA-256 - SHA-384 - SHA-512 The algorithms must be specified in upper case.
loginAttempts	The number of allowed login attempts.
email	The email address of the web user.
organization	The organization associated with the web user.
phone	The telephone number of the web user.
enabled	The web user is enabled.
approved	The web user is approved.
accountExpiresOn	The date that the web user account expires.
passwordExpirationInterval	The interval after which the web user password expires.
passwordChangedOn	The date that the web user password changed.
forcePasswordChange	Indicates whether the password must change.
servicePermissions	Indicates which services the web user has permission to access.
secureMailPermissions	Indicates that the web user can access Secure Mail.
changePasswordPermission	This option makes a Change Password link available at the top of the page in the File Transfer Portal.
lastLoginDate	The last date on which the web user logged in.

Object	Arguments
createdBy	The entity that created the web user.
createdOn	Time when the web user was created.
modifiedBy	The entity that modified the web user.
modifiedOn	Time when the web user was modified.
ipFilterEnabled	Filter access according to IP. The IP Filter can be enabled or disabled at the individual web user level.
ipFilterType	Type of IP filter. A Blacklist will deny any specified addresses and permit all others, whereas a Whitelist will only permit the specified addresses and deny all others. The following filter types are supported: - `A`. For Whitelist. - `D`. For Blacklist. - `Whitelist` - `Blacklist` The filter type is not case sensitive.
ipFilterEntries	List of IP addresses. The Filter Entries is a list of IP addresses that will either be denied or permitted based on the Filter Type selected above. The IP addresses can be entered in an array or a range format. Do not leave spaces between hyphens or slashes when specifying ranges or using CIDR notation (for example, 10.1.4.1/24 or 10.1.4.1-10.1.255.255).
generatePassword	Generate a password.
displayPassword	Display the password.
emailPassword	Provide email password.
loginMethod	Specify the login method.
loginMethodName	Name of the login method.
inactiveDays	Number of days that the web user was not active. The web user account can be disabled after a number of inactive days. Inactive days are calculated from the last login date or the last date the account was modified.
AS2Id	The ID of the sender (web user). The ID is case sensitive and can be 1 to 128 ASCII printable characters in length.
AS2SignatureAlias	This is the alias of the public certificate used by this web user to sign their messages.
AS2UploadDir	The location where messages are saved when received.
AS2WhenFileExist	The action that Managed File Transfer performs when a file with the same name already exists in the default upload folder.
AS2RequireEncryption	This option indicates whether or not messages sent by this web user must be encrypted.

Object	Arguments
AS2RequireSignature	A signed message contains a digital signature from the sender to further authenticate the message. If signatures are required, any unsigned message sent by this web user will be rejected.
AS2RequireAuthentication	Require username/password or certificate authentication for messages uploads. If authentication is not required, Managed File Transfer will use the ID to identify the web user. Informatica recommends you set the 'Require Signature' option to 'true' when authentication is not required.
AS2MdnApprovalAutomatic	If a return receipt is requested by the web user, select if the MDN will be sent automatically during the web user session or manually after the message is processed.
approvedBy	The entity that approved file send or receive.
approvedOn	Time when the file send or receive was approved.
pwdExpSentOn	The last time that a password expiration notification was sent.
maxSessions	Maximum number of sessions allowed.
inviteUserPermission	Assign permissions to invite another user to web user self-service.
invitedBy	The entity that invited the web user.
invitedOn	The time that the web user was invited.
pastExpiration	The entity has passed the expiration date.
limitTime	Limit the time period in which the web user can login.
limitTimeStart	Start of the time period in which the web user can login.
limitTimeEnd	End of the time period in which the web user can login.
limitDays	Limit time of day the web user can login.
limitDaysOfWeek	Limit which days of the week the web user can login.
viewActivityPermission	This option allows web users to view their own activity report from the Managed File Transfer File Transfer Portal. web users will be able to view their login activity, as well as audit logs on their file uploads and downloads.
goDrivePermission	This option provides web users the ability to use the Shared Drive file system for collaboration, sharing and synchronization of documents.
goDriveAccessType	When Shared Drive is enabled for the web user, you can select the web user access level.
secureFolderPermission	The Secure Folders option provides web users the ability to work with authorized network folders and files from within the browser-based File Transfer Portal.
userGoDriveDiskQuotaOption	Select whether to enable a maximum amount of disk space available for this web user in Shared Drive.

Object	Arguments
userGoDriveDiskSpace	The maximum amount of disk space available for this web user in Shared Drive.
userGoDriveDiskSpaceUnit	The unit of space used to specify the maximum amount of disk space in Shared Drive.
privateKey	Specify a private key that the web user uses.
algorithm	Specify the algorithm used with the private key.
privateKeyPassword	Specify the password for the private key.
sshKeys	List of SSH keys associated with the web user.
goDriveAccessTypeCode *	The access type code for the Shared Drive.
userGoDriveDiskSpaceUnitCode *	The disk space unit code for the Shared Drive.
* Applies only to only the	

Request Body Example

The following code shows a sample request body:

```
{
  "id": 0,
  "firstName": "John",
  "lastName": "Henry",
  "description": "Testing",
  "ghttpsAuthType": "P",
  "gas2AuthType": "P",
  "gftpesAuthType": "P",
  "gftpsAuthType": "P",
  "gsftpAuthType": "P",
  "passwordIsEncrypted": false,
  "loginAttempts": 0,
  "email": "john99@gmail.com",
  "organization": "",
  "phone": "987654321",
  "enabled": true,
  "approved": true,
  "passwordExpirationInterval": 0,
  "forcePasswordChange": false,
  "servicePermissions": 31,
  "secureMailPermissions": 1,
  "changePasswordPermission": false,
  "ipFilterEnabled": true,
  "ipFilterType": "A",
  "ipFilterEntries": [
    "10.80.223.134"
  ],
  "generatePassword": 0,
  "displayPassword": false,
  "emailPassword": false,
  "loginMethod": 101,
  "inactiveDays": 0,
  "as2Id": "",
  "as2SignatureAlias": "",
  "as2WhenFileExist": -1,
  "as2RequireEncryption": "",
  "as2RequireSignature": "",
  "as2RequireAuthentication": "",
  "as2MdnApprovalAutomatic": "",
```

```
  "maxSessions": -1,
  "inviteUserPermission": true,
  "pastExpiration": false,
  "limitTime": 0,
  "limitDays": 0,
  "limitDaysOfWeek": 0,
  "viewActivityPermission": true,
  "goDrivePermission": true,
  "goDriveAccessType": "FULLACCESS",
  "secureFolderPermission": true,
  "userGoDriveDiskQuotaOption": "NOT_SPECIFIED",
  "userGoDriveDiskSpace": 5,
  "userGoDriveDiskSpaceUnit": "GB",
  "homeDirectory": {
    "id": 0,
    "definedOnUser": false
  },
  "goDriveAccessTypeCode": "F",
  "userGoDriveDiskSpaceUnitCode": "G",
  "name": "ipw25",
  "password": "ipw$#225"
}
```

Response Body Example

The following code shows a sample response body:

```
{
    "id": 1066,
    "name": "ipw25",
    "firstName": "John",
    "lastName": "Henry",
    "description": "Testing",
    "ghttpsAuthType": "P",
    "gas2AuthType": "P",
    "gftpesAuthType": "P",
    "gftpsAuthType": "P",
    "gsftpAuthType": "P",
    "password": "ipw$#225",
    "passwordIsEncrypted": false,
    "passwordHashAlgorithm": "SHA512",
    "loginAttempts": 0,
    "email": "john99@gmail.com",
    "organization": "",
    "phone": "987654321",
    "enabled": true,
    "approved": true,
    "passwordExpirationInterval": -1,
    "forcePasswordChange": false,
    "servicePermissions": 31,
    "secureMailPermissions": 1,
    "changePasswordPermission": false,
    "createdBy": "administrator",
    "modifiedBy": "administrator",
    "ipFilterEnabled": true,
    "ipFilterType": "A",
    "ipFilterEntries": [
        {
            "value": "10.80.223.134"
        }
    ],
    "generatePassword": 0,
    "displayPassword": false,
    "emailPassword": false,
    "loginMethod": 101,
    "inactiveDays": -1,
    "as2Id": "",
    "as2SignatureAlias": "",
    "as2WhenFileExist": -1,
    "as2RequireEncryption": "",
    "as2RequireSignature": "",
```

```
    "as2RequireAuthentication": "",
    "as2MdnApprovalAutomatic": "",
    "maxSessions": -1,
    "inviteUserPermission": true,
    "homeDirectory": {
        "id": 1089,
        "definedOnUser": false
    },
    "pastExpiration": false,
    "limitTime": 0,
    "limitDays": 0,
    "limitDaysOfWeek": 0,
    "viewActivityPermission": true,
    "goDrivePermission": true,
    "goDriveAccessType": "FULLACCESS",
    "secureFolderPermission": true,
    "userGoDriveDiskQuotaOption": "NOT_SPECIFIED",
    "userGoDriveDiskSpace": 5,
    "userGoDriveDiskSpaceUnit": "GB"
}
```

Web User Count REST API

Use the **count** REST API to find the number of existing Informatica Managed File Transfer web users. This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/webusers/count
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON to the REST API call. The following table describes the response body objects:

Object	Arguments
firstResult	Specify the first result to present.
maxResults	Specify the maximum number of results to present.
selectedSortColumn	Select which column is used to sort the resource information.
sortAscending	Sort the resources in ascending order.
matchAll	Provide all the matches to the search expression when performing the search.
useExactMatch	Exactly match the search expression when performing the search.
simpleSearchString	Use a simple search string to perform the search.
simpleSearch	Use a simple search to perform the search.

Object	Arguments
searchString	Specify the search string used to perform the search.
webUserNames	List of web user names to search for.

Request Body Example

The following code shows a sample request body:

```
{
 "firstResult":0,
 "maxResults":10,
 "selectedSortColumn":0,
 "sortAscending":true,
 "matchAll":true,
 "useExactMatch":false,
 "simpleSearchString":"Test",
 "simpleSearch":false,
 "searchString":null,
 "webUserNames":null,
 "markExisting":false
}
```

Response Body Example

The following code shows a response body:

```
3
```

Find Web User REST API

Use the **search** REST API to find an Informatica Managed File Transfer web user using a search expression. This API uses the POST method.

Use the following URL for the REST API call:

```
POST http://<hostName>:<portNumber>/informaticamft/api/v1/webusers/search
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON format. The following table describes the request body objects:

Object	Arguments
firstResult	Specify the first result to present.
maxResults	Specify the maximum number of results to present.
selectedSortColumn	Select which column is used to sort the resource information.
sortAscending	Sort the resources in ascending order.
matchAll	Provide all the matches to the search expression when performing the search.

Object	Arguments
useExactMatch	Exactly match the search expression when performing the search.
simpleSearchString	Use a simple search string to perform the search.
simpleSearch	Use a simple search to perform the search.
searchString	Specify the search string used to perform the search.
webUserNames	List of web user names to search for.

The following table describes the response body objects:

Object	Arguments
id	Specify the web user identification number.
name	User name of the web user.
firstName	First name of the web user.
lastName	Last name of the web user.
emailId	The email address of the web user.
status	Status of the web user.
organization	Organization associated with the web user.

Request Body Example

The following code shows a sample request body:

```
{
      "firstResult":0,
     "maxResults":70,
     "selectedSortColumn":0,
     "sortAscending":true,
     "matchAll":true,
     "useExactMatch":true,
     "simpleSearchString":"test",
     "simpleSearch":true,
     "searchString":null,
     "webUserNames":null
}
```

Response Body Examples

The following code shows a response body:

```
[
    {
        "id": 1052,
        "username": "Monitor_Test",
        "firstName": "",
        "lastName": "",
        "emailId": "",
        "status": "Enabled",
        "organization": ""
    },
```

```
    {
        "id": 1053,
        "username": "Monitor_Test_batch_hosted",
        "firstName": "",
        "lastName": "",
        "emailId": "",
        "status": "Enabled",
        "organization": ""
    },
    {
        "id": 1001,
        "username": "test",
        "firstName": "",
        "lastName": "",
        "emailId": "",
        "status": "Enabled",
        "organization": ""
    }
]
```

Find Web User by ID REST API

Use the **userId** REST API to find an Informatica Managed File Transfer web user by an identification number. This API uses the GET method.

Use the following URL for the REST API call:

```
GET http://<hostName>:<portNumber>/informaticamft/api/v1/webusers/{userId}
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

The following table describes the request variable:

Object	Arguments
userId	The database ID of the web user.

The following table describes the response body objects:

Object	Arguments
id	Specify the resource identification number.
name	User name of the web user.
firstName	First name of the web user.
lastName	Last name of the web user.
description	Description of the web user.
password	The password associated with the web user.

Object	Arguments
passwordIsEncrypted	Indicates whether or not the password is encrypted.
passwordHashAlgorithm	Indicates whether or not the password is encrypted with a hash algorithm. Supported hash algorithms are MD2, MD5, SHA-1, SHA-256, SHA-384 and SHA-512. The algorithms must be specified in upper case.
fingerprint	Fingerprint associated with the web user.
loginAttempts	The number of allowed login attempts.
email	The email address of the web user.
organization	The organization associated with the web user.
phone	The telephone number of the web user.
enabled	The web user is enabled.
approved	The web user is approved.
accountExpiresOn	The date that the web user account expires.
passwordExpirationInterval	The interval after which the web user password expires.
passwordChangedOn	The date that the web user password changed.
forcePasswordChange	Indicates whether the password must change.
servicePermissions	Indicates which services the web user has permission to access.
secureMailPermissions	Indicates that the web user can access Secure Mail.
changePasswordPermission	This option makes a Change Password link available at the top of the page in the File Transfer Portal for members of the Web User Group.
lastLoginDate	The last date on which the web user logged in.
createdBy	The entity that created the web user.
createdOn	Time when the web user was created.
modifiedBy	The entity that modified the web user.
modifiedOn	Time when the web user was modified.
ipFilterEnabled	Filter access according to IP. The IP Filter can be enabled or disabled at the individual Web User level.
ipFilterType	Type of IP filter. A Blacklist will deny any specified addresses and permit all others, whereas a Whitelist will only permit the specified addresses and deny all others.
ipFilterEntries	List of IP addresses. The Filter Entries is a list of IP addresses that will either be denied or permitted based on the Filter Type selected above.

Object	Arguments
generatePassword	Generate a password.
displayPassword	Display the password.
emailPassword	Provide email password.
loginMethod	Specify the login method.
loginMethodName	Name of the login method.
inactiveDays	Number of days that the web user was not active. The Web User account can be disabled after a number of inactive days. Inactive days are calculated from the last login date or the last date the account was modified.
AS2Id	The ID of the sender (Web User). The ID is case sensitive and can be 1 to 128 ASCII printable characters in length.
AS2SignatureAlias	This is the alias of the public certificate used by this Web User to sign their messages. If
AS2UploadDir	The location where messages are saved when received.
AS2WhenFileExist	The action that Managed File Transfer performs when a file with the same name already exists in the default upload folder.
AS2RequireEncryption	This option indicates whether or not messages sent by this Web User must be encrypted.
AS2RequireSignature	A signed message contains a digital signature from the sender to further authenticate the message. If signatures are required, any unsigned message sent by this Web User will be rejected.
AS2RequireAuthentication	Require username/password or certificate authentication for messages uploads. If authentication is not required, Managed File Transfer will use the ID to identify the Web User. Informatica recommends you set the 'Require Signature' option to 'true' when authentication is not required.
AS2MdnApprovalAutomatic	If a return receipt is requested by the Web User, select if the MDN will be sent automatically during the Web User's session or manually after the message is processed.
HTTPSFingerprint	If the specified Web User Template has the Authentication Type for HTTPS set to Certificate or Either, the HTTPSFingerprint column is required.
AS2Fingerprint	If the specified Web User Template has the Authentication Type for AS2 set to Certificate, Either, or Certificate and Password, the AS2Fingerprint column is required.
FTPESFingerprint	If the specified Web User Template has the Authentication Type for FTPES set to Certificate, Either or Certificate and Password, the FTPESFingerprint column is required.
FTPSFingerprint	If the specified Web User Template has the Authentication Type for FTPS set to Certificate, Either or Certificate and Password, the FTPSFingerprint column is required.

Object	Arguments
approvedBy	The entity that approved file send or receive.
approvedOn	Time when the file send or receive was approved.
pwdExpSentOn	The last time that a password expiration notification was sent.
maxSessions	Maximum number of sessions allowed.
inviteUserPermission	Assign permissions to invite another user to web user self-service.
invitedBy	The entity that invited the web user.
invitedOn	The time that the web user was invited.
pastExpiration	The entity has passed the expiration date.
limitTime	Limit the time period in which the Web User can login.
limitTimeStart	Start of the time period in which the Web User can login.
limitTimeEnd	End of the time period in which the Web User can login.
limitDays	Limit time of day the Web User can login.
limitDaysOfWeek	Limit which days of the week the Web User can login.
viewActivityPermission	This option allows Web Users to view their own activity report from the Managed File Transfer File Transfer Portal. Web Users will be able to view their login activity, as well as audit logs on their file uploads and downloads.
goDrivePermission	This option provides Web Users the ability to use the Shared Drive file system for collaboration, sharing and synchronization of documents.
goDriveAccessType	When Shared Drive is enabled for the Web User, you can select the Web User access level.
secureFolderPermission	The Secure Folders option provides Web Users the ability to work with authorized network folders and files from within the browser-based File Transfer Portal.
userGoDriveDiskQuotaOption	Select whether to enable a maximum amount of disk space available for this Web User in Shared Drive.
userGoDriveDiskSpace	The maximum amount of disk space available for this Web User in Shared Drive.
userGoDriveDiskSpaceUnit	The unit of space used to specify the maximum amount of disk space in Shared Drive.
privateKey	Specify a private key that the web user uses.
algorithm	Specify the algorithm used with the private key.
privateKeyPassword	Specify the password for the private key.
sshKeys	List of SSH keys associated with the web user.

Object	Arguments
goDriveAccessTypeCode	The access type code for the Shared Drive.
userGoDriveDiskSpaceUnitCode	The disk space unit code for the Shared Drive.

Response Body Examples

The following code shows a response body:


```
{
    "id": 1046,
    "name": "ipw1234172",
    "firstName": "",
    "lastName": "",
    "description": "",
    "ghttpsAuthType": "P",
    "gas2AuthType": "P",
    "gftpesAuthType": "P",
    "gftpsAuthType": "P",
    "gsftpAuthType": "P",
    "password": " /reoVbQpbE9YJBGtRm3NivBA==",
    "passwordIsEncrypted": true,
    "passwordHashAlgorithm": "SHA512",
    "loginAttempts": 0,
    "email": "",
    "organization": "",
    "phone": "",
    "enabled": true,
    "approved": true,
    "passwordExpirationInterval": -1,
    "passwordChangedOn": 1613730897203,
    "forcePasswordChange": false,
    "servicePermissions": 31,
    "secureMailPermissions": 1,
    "changePasswordPermission": false,
    "createdBy": "administrator",
    "createdOn": 1613730897203,
    "modifiedBy": "administrator",
    "modifiedOn": 1613730897203,
    "ipFilterEnabled": false,
    "ipFilterType": "D",
    "ipFilterEntries": [
        {
            "value": "2405:201:d01c:2002::c0a8:1d01"
        }
    ],
    "generatePassword": 0,
    "displayPassword": false,
    "emailPassword": false,
    "loginMethod": 101,
    "inactiveDays": -1,
    "as2Id": "",
    "as2SignatureAlias": "",
    "as2WhenFileExist": -1,
    "as2RequireEncryption": "",
    "as2RequireSignature": "",
    "as2RequireAuthentication": "",
    "as2MdnApprovalAutomatic": "",
    "maxSessions": -1,
    "inviteUserPermission": true,
    "homeDirectory": {
        "id": 1068,
        "definedOnUser": true
    },
    "pastExpiration": false,
    "limitTime": 0,
```

```
    "limitDays": 0,
    "limitDaysOfWeek": 0,
    "viewActivityPermission": true,
    "goDrivePermission": true,
    "goDriveAccessType": "FULLACCESS",
    "secureFolderPermission": true,
    "userGoDriveDiskQuotaOption": "NOT_SPECIFIED",
    "userGoDriveDiskSpace": 5,
    "userGoDriveDiskSpaceUnit": "GB",
    "sshKeys": []
}
```

Update Web User REST API

Use the **userId** REST API to update an Informatica Managed File Transfer web user. This API uses the PUT method.

Use the following URL for the REST API call:

```
PUT http://<hostName>:<portNumber>/informaticamft/api/v1/webusers/{userId}
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.
- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

You can provide a request body in JSON to the REST API call. The following table describes the response body objects:

Object	Arguments
id	Specify the resource identification number.
name	User name of the web user.
firstName	First name of the web user.
lastName	Last name of the web user.
description	Description of the web user.
password	The password associated with the web user.
passwordIsEncrypted	Indicates whether or not the password is encrypted.
passwordHashAlgorithm	Indicates whether or not the password is encrypted with a hash algorithm. Supported hash algorithms are MD2, MD5, SHA-1, SHA-256, SHA-384 and SHA-512. The algorithms must be specified in upper case.
loginAttempts	The number of allowed login attempts.
email	The email address of the web user.
organization	The organization associated with the web user.
phone	The telephone number of the web user.

Object	Arguments
enabled	The web user is enabled.
approved	The web user is approved.
passwordExpirationInterval	The interval after which the web user password expires.
forcePasswordChange	Indicates whether the password must change.
servicePermissions	Indicates which services the web user has permission to access.
secureMailPermissions	Indicates that the web user can access Secure Mail.
changePasswordPermission	This option makes a Change Password link available at the top of the page in the File Transfer Portal for members of the Web User Group.
createdBy	The entity that created the web user.
createdOn	Time when the web user was created.
modifiedBy	The entity that modified the web user.
ipFilterEnabled	Filter access according to IP. The IP Filter can be enabled or disabled at the individual Web User level.
ipFilterType	Type of IP filter. A Blacklist will deny any specified addresses and permit all others, whereas a Whitelist will only permit the specified addresses and deny all others.
ipFilterEntries	List of IP addresses. The Filter Entries is a list of IP addresses that will either be denied or permitted based on the Filter Type selected above.
generatePassword	Generate a password.
displayPassword	Display the password.
emailPassword	Provide email password.
loginMethod	Specify the login method.
inactiveDays	Number of days that the web user was not active. The Web User account can be disabled after a number of inactive days. Inactive days are calculated from the last login date or the last date the account was modified.
AS2Id	The ID of the sender (Web User). The ID is case sensitive and can be 1 to 128 ASCII printable characters in length.
AS2SignatureAlias	This is the alias of the public certificate used by this Web User to sign their messages. If
AS2WhenFileExist	The action that Managed File Transfer performs when a file with the same name already exists in the default upload folder.
AS2RequireEncryption	This option indicates whether or not messages sent by this Web User must be encrypted.

Object	Arguments
AS2RequireSignature	A signed message contains a digital signature from the sender to further authenticate the message. If signatures are required, any unsigned message sent by this Web User will be rejected.
AS2RequireAuthentication	Require username/password or certificate authentication for messages uploads. If authentication is not required, Managed File Transfer will use the ID to identify the Web User. Informatica recommends you set the 'Require Signature' option to 'true' when authentication is not required.
AS2MdnApprovalAutomatic	If a return receipt is requested by the Web User, select if the MDN will be sent automatically during the Web User's session or manually after the message is processed.
maxSessions	Maximum number of sessions allowed.
inviteUserPermission	Assign permissions to invite another user to web user self-service.
pastExpiration	The entity has passed the expiration date.
limitTime	Limit the time period in which the Web User can login.
limitDays	Limit time of day the Web User can login.
limitDaysOfWeek	Limit which days of the week the Web User can login.
viewActivityPermission	This option allows Web Users to view their own activity report from the Managed File Transfer File Transfer Portal. Web Users will be able to view their login activity, as well as audit logs on their file uploads and downloads.
goDrivePermission	This option provides Web Users the ability to use the Shared Drive file system for collaboration, sharing and synchronization of documents.
goDriveAccessType	When Shared Drive is enabled for the Web User, you can select the Web User access level.
secureFolderPermission	The Secure Folders option provides Web Users the ability to work with authorized network folders and files from within the browser-based File Transfer Portal.
userGoDriveDiskQuotaOption	Select whether to enable a maximum amount of disk space available for this Web User in Shared Drive.
userGoDriveDiskSpace	The maximum amount of disk space available for this Web User in Shared Drive.
userGoDriveDiskSpaceUnit	The unit of space used to specify the maximum amount of disk space in Shared Drive.

Request Body Example

The following code shows a sample request body:

```
{
  "id": 1066,
    "name": "ipw25",
    "firstName": "John",
    "lastName": "Fords",
    "description": "TestingMethod",
    "ghttpsAuthType": "P",
    "gas2AuthType": "P",
```

```
    "gftpesAuthType": "P",
    "gftpsAuthType": "P",
    "gsftpAuthType": "P",
    "password": "ipw$#2259",
    "passwordIsEncrypted": false,
    "passwordHashAlgorithm": "SHA512",
    "loginAttempts": 0,
    "email": "john99@gmail.com",
    "organization": "",
    "phone": "9876754321",
    "enabled": true,
    "approved": true,
    "passwordExpirationInterval": -1,
    "forcePasswordChange": false,
    "servicePermissions": 31,
    "secureMailPermissions": 1,
    "changePasswordPermission": false,
    "createdBy": "administrator",
    "modifiedBy": "administrator",
    "ipFilterEnabled": true,
    "ipFilterType": "A",
    "ipFilterEntries": [
        {
            "value": "10.0.223.134"
        }
    ],
    "generatePassword": 0,
    "displayPassword": false,
    "emailPassword": false,
    "loginMethod": 101,
    "inactiveDays": -1,
    "as2Id": "",
    "as2SignatureAlias": "",
    "as2WhenFileExist": -1,
    "as2RequireEncryption": "",
    "as2RequireSignature": "",
    "as2RequireAuthentication": "",
    "as2MdnApprovalAutomatic": "",
    "maxSessions": -1,
    "inviteUserPermission": true,
    "homeDirectory": {
        "id": 1089,
        "definedOnUser": false
    },
    "pastExpiration": false,
    "limitTime": 0,
    "limitDays": 0,
    "limitDaysOfWeek": 0,
    "viewActivityPermission": true,
    "goDrivePermission": true,
    "goDriveAccessType": "FULLACCESS",
    "secureFolderPermission": true,
    "userGoDriveDiskQuotaOption": "NOT_SPECIFIED",
    "userGoDriveDiskSpace": 5,
    "userGoDriveDiskSpaceUnit": "GB"
}
```

Response Body Examples

The following code shows a response body:

```
{
    "id": 1066,
    "name": "ipw25",
    "firstName": "John",
    "lastName": "Fords",
    "description": "TestingMethod",
    "ghttpsAuthType": "P",
    "gas2AuthType": "P",
    "gftpesAuthType": "P",
    "gftpsAuthType": "P",
```

```
    "gsftpAuthType": "P",
    "password": "ipw$#2259",
    "passwordIsEncrypted": false,
    "passwordHashAlgorithm": "SHA512",
    "loginAttempts": 0,
    "email": "john99@gmail.com",
    "organization": "",
    "phone": "9876754321",
    "enabled": true,
    "approved": true,
    "passwordExpirationInterval": -1,
    "forcePasswordChange": false,
    "servicePermissions": 31,
    "secureMailPermissions": 1,
    "changePasswordPermission": false,
    "createdBy": "administrator",
    "modifiedBy": "administrator",
    "ipFilterEnabled": true,
    "ipFilterType": "A",
    "ipFilterEntries": [
        {
            "value": "10.80.223.134"
        }
    ],
    "generatePassword": 0,
    "displayPassword": false,
    "emailPassword": false,
    "loginMethod": 101,
    "inactiveDays": -1,
    "as2Id": "",
    "as2SignatureAlias": "",
    "as2WhenFileExist": -1,
    "as2RequireEncryption": "",
    "as2RequireSignature": "",
    "as2RequireAuthentication": "",
    "as2MdnApprovalAutomatic": "",
    "maxSessions": -1,
    "inviteUserPermission": true,
    "homeDirectory": {
        "id": 1097,
        "definedOnUser": true
    },
    "pastExpiration": false,
    "limitTime": 0,
    "limitDays": 0,
    "limitDaysOfWeek": 0,
    "viewActivityPermission": true,
    "goDrivePermission": true,
    "goDriveAccessType": "FULLACCESS",
    "secureFolderPermission": true,
    "userGoDriveDiskQuotaOption": "NOT_SPECIFIED",
    "userGoDriveDiskSpace": 5,
    "userGoDriveDiskSpaceUnit": "GB"
}
```


Delete Web User REST API

Use the **userId** REST API to delete an Informatica Managed File Transfer web user. This API uses the DELETE method.

Use the following URL for the REST API call:

```
DELETE http://<hostName>:<portNumber>/informaticamft/api/v1/webusers/{userId}
```

- `<hostName>` is the host name or IP address of the Managed File Transfer server.

- `<portNumber>` is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, `http://myserver:8000` or `https://myserver:8002`.

INDEX