



QUICK START GUIDE

Version 6.0.0

1.0	Pre-requisites	3
1.1	Database Requirements	3
1.2	Server Requirements	3
1.3	Client Computer	3
1.4	Account Permissions	3- 4
2.0	Installation	4
2.1	Install BitTruster Server	4- 5- 6
3.0	Configuring BitTruster	6- 7- 8- 9
3.1	E-Mail Server Settings	9
3.2	Test email configuration	9
3.3	Configuring Active Directory Sync	10
3.4	Preparing the client computer	10
3.5	Check communication to the client computer	10
3.6	Encrypting a computer with “TPM only” Protection	10- 11
3.7	Encrypting a computer with “TPM+PIN” Protection	11
4.0	Recovery	11-12
4.1	Recovering PIN or Passphrase in the Self-help Portal	12
4.2	Changing PIN or Passphrase in the Self-help Portal	12- 13
4.3	Decrypting a computer	13
5.0	APPENDIX Troubleshooting	13
5.1	Error 2147023174 RPC Client not available.	13- 14
5.2	Troubleshooting -999 Access denied	14-15

1. Prerequisites

1.1. Server requirements: Windows Server 2008 R2 or higher.

- RAM: 2 GB
- Disk Space: 1 GB
- CPU: dual-core

CPU Installation on virtual machines supported internal mail server recommended for reporting and user notifications.

Note: We recommend installing the BitTruster Server on a member server, not on a Domain Controller. If you need to run the installation on a Domain Controller, please make sure that a SQL Server is already installed, as the BitTruster installation package will fail to install with an integrated SQL database.

1.2. Database requirements:

Microsoft SQL Server R2 or higher. (SQL Express supported).

As BitTruster v-6.0.0 does not provide an integrated SQL server, the client must first install SQL server R2 / Express before installing BT v6.0.0.

1.3. Client Computer:

- Windows 7 Enterprise
- Windows 8/8.1 Pro or Enterprise
- Windows 10 Pro or Enterprise

Windows 2008 or later Make sure TPM is available on the test computer. BitTruster is capable of managing and enabling the TPM chip remotely as long as it is enabled in the BIOS/UEFI settings. If the computer has no TPM chip available, you can run the evaluation enabling Passphrase protection instead of TPM.

Note: Passphrase Protection is only available for Windows 8 and Windows 10, Windows 2012 and 2016.

1.4. Account Permissions:

Domain account, local admin on the test server, local admin on the test clients, permission to create and assign GPOs.

BitTruster recommends running the evaluation in a Test/Evaluation environment where you have full control to make ad-hoc changes where needed.

2. Installation:

Download the installation package from the download link you have received from BitTruster. If you do not have a download link, send an email to support@BitTruster.com or go to www.BitTruster.com to request a download link.

The installation package includes BitTruster and provides all configurations you need to evaluate BitTruster.

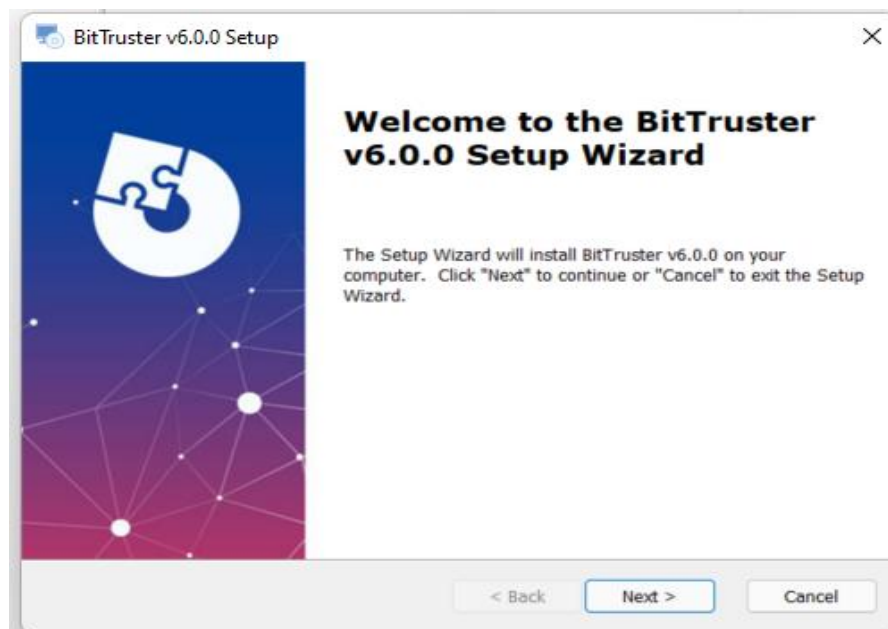
2.1. Install BitTruster Server

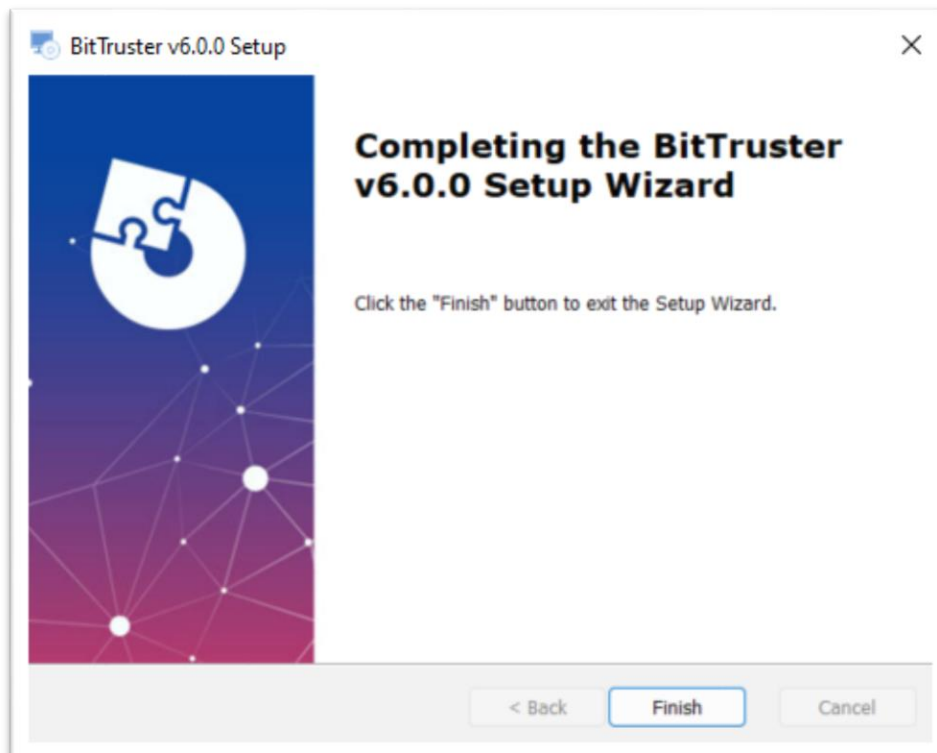
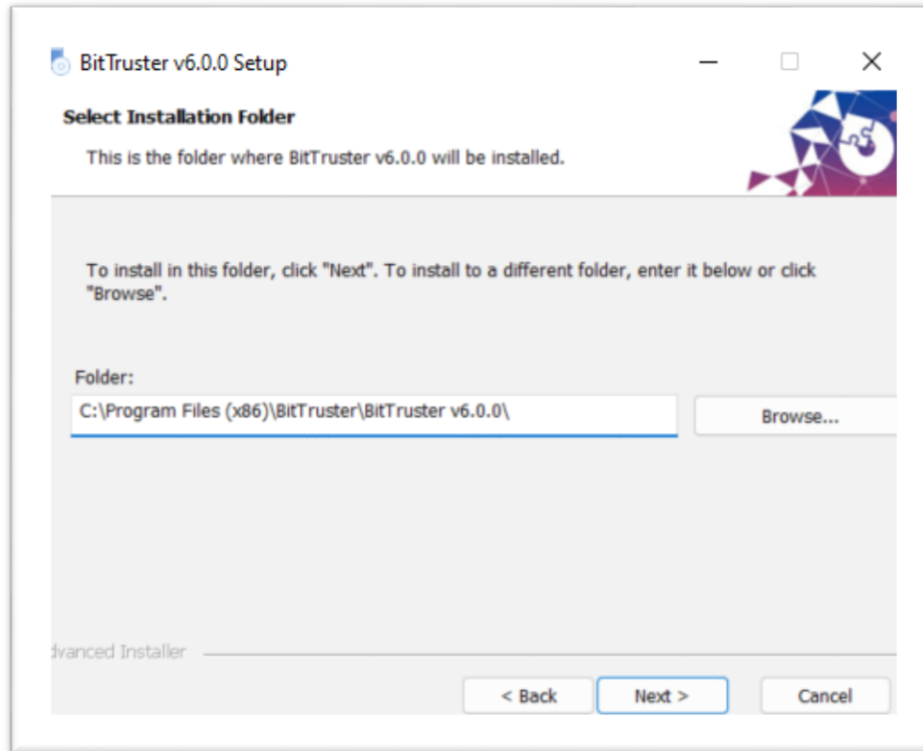
To install BitTruster v-6.0.0. Follow the steps below:

Note: First, we recommend new users to install the Microsoft SQL Server.

Step-1: Run Installation Package

Run the Install-Package as administrator and follow the wizard instructions:





Step-2: Run Database Scripts.

- Please run the DB creation scripts from “[BT Installation directory]/_config/DBCreation.sql” for a fresh BitTruster v-6.0.0 installation.
- Please run the DB upgrade scripts from “[BT Installation directory]/_config/DBChanges.sql” on your existing BT database, if you are upgrading from BT v-5.x.

Note:

- ❖ All BitTruster services in service.msc are disabled by default after installation; the client must first complete the appropriate settings and then manually start all services as described in this document.
- ❖ BitTruster requires GPO policy to be in place. Please, import two required GPO policies from [BT Installation directory]/_config/GroupPolicyObjects

The user should proceed with the BitTruster configuration process after the successful completion of the installation steps.

3. Configuring BitTruster

On the successful Installation of BitTruster v-6.0.0

Step-1 - Define Connection to Database (Link database)

As BitTruster v-6.0.0 does not come up with an Integrated SQL Server and the client has installed the SQL Server manually. Therefore, the client is required to define the connection string to the SQL Server.

- Please make sure that the default connection of the connection string is updated. To do that, go to the **AppSetting.json** in the BitTruster installation directory. i.e., “[BitTruster Installation directory]\BitTruster\BitTruster v6.0.0_config”.
- In the DomainKey of the AppSetting.json file, the user must give the domain connection/machine name. Semi-colon separators must be used to separate multiple domain connections/machine names.

```

1  {
2      "AllowedHosts": "*",
3      "ConnectionStrings": {
4          "DefaultConnection": "Data Source=[serverIP];Initial Catalog=[DatabaseName]; User ID=[];Passw
5          "AppKey": "fromFrontEnd",
6          "standardDomainName": "false",
7          "DomainKey": "firstDomain; secondDomain; thirdDomain",
8          "logLocation": "C:\\Program Files (x86)\\Bit Truster\\Logs\\SHP\\"
9      },

```

Step-2 – Firewall Enablement

After the installation of BitTruster v-6.0.0, the user is required to open two communication ports (1535, 1536) on the firewall by defining the inbound rules.

Step-4 – Update server IP / host in configurations.

After defining ports on firewall in order to let front-end communicate with backend API's we need to update API endpoint's by replacing localhost with server IP / Hostname in configuration file which is located at path "C:\Program Files (x86)\BitTruster\BitTruster v6.0.0\frontendapp\managementapp\assets\appConfig.json"

- "apiBTManagementBaseUrl": "<https://localhost:1535/api/>"
- "apiSHPBaseUrl": "<https://localhost:1536/api/>"

Note: The client is required to replace localhost with the IP address or hostname of the installation server. In order to connect to the BT v-6.0.0 backend across a network. i.e., [https://\[IP/Host\]/api](https://[IP/Host]/api)

Step-3 – Certificate Configurations

To run firewall ports over HTTPS, the user must configure the certificate. Users will configure certificates on their own or through a third party, and the path of the certificate will be linked in the AppSetting.json file.

1. The front-end certificate can be configured using the TomCat server file.
i.e., [BitTruster Installation
directory]\BitTruster\BitTrusterv6.0.0\frontendapp\conf\server.xml
2. Backend certificate configuration can be done in Kestrel_Management and Kestrel_SHP.

```

{
  "Kestrel_Managment": {
    "Endpoints": {
      "Http": {
        "Url": "http://*:1533"
      },
      "HttpsInlineCertFile": {
        "Url": "https://*:1535",
        "Certificate": {
          "Path": "C:\\tmp\\localhost.pfx",
          "Password": "P@ssw0rd!"
        }
      },
      "HttpsDefaultCert": {
        "Url": "https://*:1501"
      }
    },
    "Certificates": {
      "Default": {
        "Path": "C:\\tmp\\localhost.pfx",
        "Password": "P@ssw0rd!"
      }
    }
  },
  "Kestrel_SHP": {
    "Endpoints": {
      "Http": {
        "Url": "http://*:1534"
      },
      "HttpsInlineCertFile": {
        "Url": "https://*:1536",
        "Certificate": {
          "Path": "C:\\tmp\\localhost.pfx",
          "Password": "P@ssw0rd!"
        }
      },
      "HttpsDefaultCert": {
        "Url": "https://*:1500"
      }
    }
  }
}

```

Step-4 – Define admin credentials to services.

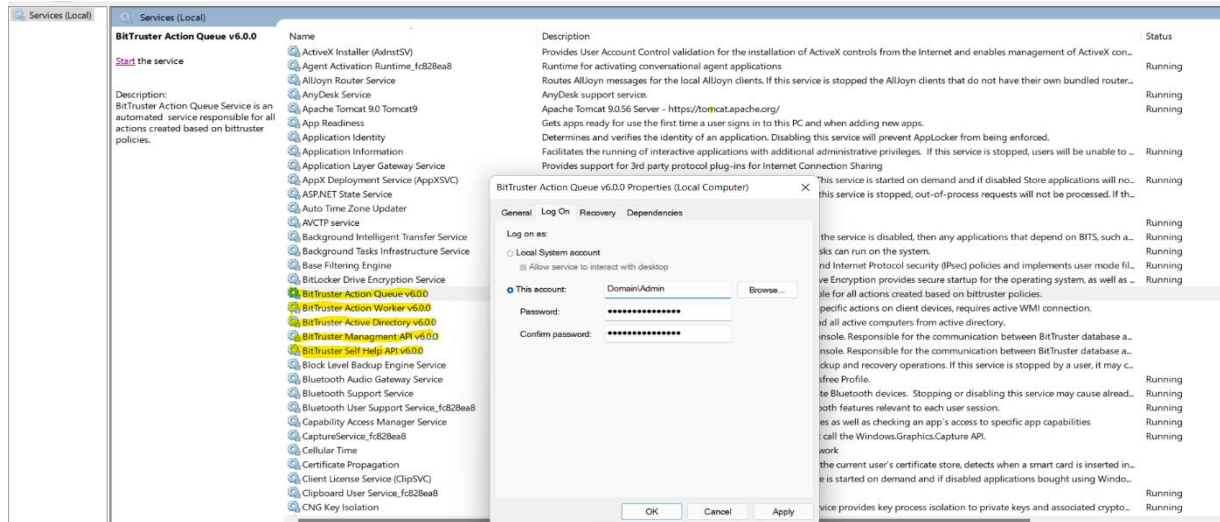
BitTruster v-6.0.0 creates three window services and two web api's after installation. Define the admin credentials in the log-on tab of all BitTruster v-6.0.0 services, in services.msc. Windows Services

- Active Directory Worker
- Action Queue Worker
- Action Worker

Web Api's:

- BitTruster Management
- BitTruster Self Help

QUICK START GUIDE



BitTruster Management and BitTruster Self Help are two web apps on the web application server.

Note: The user must refresh the web pages in order to use the applications.

Use the BitTruster Management API and the BitTruster Self Help API for the first time.

3.1. E-Mail Server Settings

BitTruster leverages email to send out notifications like PIN changes, passphrase changes, reports, or TPM notifications to inform end-user and administrators. To configure the email settings please change to the Settings tab from the navigation pane and select Email service in the top menu. Configure the email address that should be used to send emails to the users. Add a new E-Mail Server entry with appropriate credentials which are allowed to send out emails. Click on Save when finished with the configuration.

3.2. Test email configuration

To check if the email settings have been applied correctly, you can also use the “Test” button beside the Email Server configuration. Just simply click on “Test” and wait for the “Send test email?” pop-up screen. Check if the email is correct and click on “Yes”. You should see the notification “Email has been sent successfully”.

3.3. Configuring Active Directory Sync

To import new computers to the Management Console BitTruster needs to be configured to import new computer objects from Active Directory. For this, you can create a new AD-Connector.

Select “Synchronize” from the left navigation pane. Click “+” in “AD Import Paths” to add a new AD-Connector.

On the right side in the “AD Path Selection” section select the Organizational Unit that you want to import. Once you have selected the OU the LDAP path in the “Settings” section will change. Click on “Save”.

BitTruster will now import the computer objects from the configured OU. This can take a few minutes. Go back to the Dashboard view. You should now see your OU and the corresponding computers in the dashboard overview.

3.4. Preparing the client computer

Log on to a client with an AD user that has an email address.

The client should be part of the OU that has been imported into BitTruster before. Open the TPM console (tpm.msc) as an administrator and check if the TPM is turned on and ready for use.

If the TPM is not shown in the TPM console please check in BIOS if the TPM has been disabled. Ensure that you log on interactively (no RDP session) otherwise the user is not added to the user's list.

3.5. Check communication to the client computer

Execute the BTclientconnect scripts from [BitTruster Installation directory]/_config/BTclientconnect.vbs to ensure that the BitTruster server can communicate with clients.

3.6. Encrypting a computer with “TPM only” Protection

Once the BitTruster Server established communication to the client you can now continue to prepare an encryption policy.

On the Management Center go to Dashboard and select the computer that you have prepared for testing. Once clicked you can see the detail view for this computer on the right side. Select “Policy” and change the setting from “Auto” to “Manual”. Select the policy for “manual TPM only” encryption.

Click on “Save”. The computer should start to encrypt after it has received the new policy. You can view progress in the Action Queue of the computer: Click on the computer in the Dashboard and select “Actions” on the right detail pane. You can now see the action status of the selected computer.

Note: If you are receiving an 8-character passphrase at this point your TPM chip might not be configured correctly or is deactivated. Please check if it is turned on and enabled in the BIOS, if that’s done BitTruster will automatically switch to the more secure TPM+PIN state.

3.7. Encrypting a computer with “TPM+PIN” Protection

In the Management Center go to Dashboard and select the computer that you have prepared for testing. Once clicked you can see the detail view for this computer on the right side.

Select “Policy” and change the setting from “Auto” to “Manual”.

Select the policy for “manual TPM+PIN” encryption.

You can do this while the computer is still encrypting. You don’t need to wait until the encryption is finished. Click on “Save”. You should receive a notification email from BitTruster with your new 6-digit PIN number

Reboot the computer. You will be prompted to type in your PIN before the computer continues to boot up. Type in the PIN Number and press “Enter”.

4. Recovery

Recovering PIN or Passphrase in the Management Center

If the user forgets the PIN or Passphrase of his computer, you can easily recover this information in Management Center.

Go to the Management Center and select “Recovery” from the navigation pane on the left. Type in the first letters of the computer that want to recover. If you only have the ProtectorIdentifier you need to change the search option in the search pane.

Once you selected the computer you see the computer information and the recovery options. BitTruster shows only the recovery options which are available for this computer. In our example, the computer should now be protected with a PIN.

Click on the “Email” button in the “TPM+PIN” section. The “Send PIN” message pops up to inform you that an email has been sent out. BitTruster sends an email to all users that are assigned to this computer.

Please verify that you have received the email with the PIN notification. If the user is unable to receive emails you can use the “Show” option to tell him the PIN on the phone or any other way of communication. Click on “Show” in the “TPM+PIN” section. The “TPM+PIN” message pops up with the corresponding PIN for this computer.

Note: When using “Show” option for any of the recovery sections BitTruster will trigger a change of the recovery information once for the next time it establishes a connection to the client computer. For PIN and Passphrase, the users will be informed about the new login information via email once it has been changed.

Recovery key are always changed on usage, but will not trigger a notification.

4.1. Recovering PIN or Passphrase in the Self Help Portal

BitTruster offers a Self-Help Portal where users can log in with their Active Directory credentials and do some recovery steps on their own but also change their login information (PIN/Passphrase) without interacting with the helpdesk.

Open an internet browser from another computer and type in:

<https://\HostameOfYourBitTrusterServer>.

If you don't know the correct URL of the Self Help Portal open the Self Help Portal from the BitTruster Server (icon on the desktop) and check the URL.

Login in with your Active Directory credentials.

Please note that the Self Help Portal only accepts logins from BitTruster users even if the login information is correct. Once logged in you should now see all the computers that are assigned to you. Select the computer that you want to recover. Click on “Show PIN” and approve that you want to see the PIN. You should now see the PIN of your computer. Please note that BitTruster is not changing the PIN of your computer after you used “Shown PIN” in the Self Help Portal.

Note: BitTruster is using a Self-Signed Certificate per default. We recommend replacing this with a certificate from an internal CA.

4.2. Changing PIN or Passphrase in the Self Help Portal

The Self Help Portal also allows users to change their PIN or Passphrase without interacting with the Help Desk.

Please login to the SelfHelp Portal on the computer where you want to change the PIN or Passphrase. The computer must be able to be contacted by the BitTruster Server. Click on the

computer in the SelfHelp Portal and select the “Change PIN” option. Type in your new PIN and click on “Set PIN”. Your PIN will now be changed and can be used on the next boot login.

4.3. Decrypting a computer

In the Management Center go to Dashboard and select the computer that you have prepared for testing. Once clicked you can see the detail view for this computer on the right side. Select “Policy” and change the setting from “Auto” to “Manual”. Select the policy for “manual decrypt” encryption. Click on “Save”. The computer should start to decrypt after it has received the new policy. To view progress, you can check the Action Queue of this machine.

5. APPENDIX Troubleshooting

5.1. Error 2147023174 RPC Client not available.

BitTruster uses WMI to connect to clients. When receiving the error code -2147023174 it means that BitTruster could not connect to the client. This can have multiple reasons. Most of the time the client is offline and BitTruster will connect the next time the client is online.

However, it's also possible that there are other reasons why the connection fails. If the request just times out there's no reply which would allow providing a more detailed error message. The same applies to firewalls, as firewalls - for good reasons - do not tell the questioning party that a package has been dropped it looks like a timeout.

Issues that do **NOT** cause this issue:

Permissions - When a user is not having the required permissions BitTruster will show an appropriate error message.

DNS record pointing to a different client - When the DNS server points to a different machine than the actual client BitTruster will show a meaningful error message.

Note this only applies if the DNS record points to a different client that is actually online. DNS is most of the time the root cause for this error.

To analyze the issue, follow these steps:

- **Verify that the client is online and in a network segment that can be reached by the BitTruster server.**
- **Check DNS**
 - Ensure you run the following commands from the BitTruster server

- Ping the client using the FQDN, do not just use the hostname it can return the different IP address in rare situations

- Verify that the returned IP matches the client IP

- **Check Firewall**

- When the DNS server returns the correct IP ensure that the Windows Firewall from the client accepts WMI in

- Execute the following WMI command using the FQDN of the client:

- `wmic /NODE:<clientname> /USER:<yourdomain\administrator> OS GET Name`

- When using the Windows firewall ensure that the "BitTruster - Firewall settings" GPO has been applied to the correct OU and the client already retrieved the GPO

- **Verify if the NETBIOS name is correct:**

- open a cmd prompt and run the following command:

- `nbtstat -n`

- check the output for NETBIOS name where the Type = GROUP and Status = Registered

- verify that you have the same NETBIOS entry in AD-Sync configuration in the BitTruster Management

- **Verify the default gateway to ensure that the BitTruster server has a route to the client and vice versa.**

- From the BitTruster Server

- `tracert`

- From the client

- `tracert`

5.2. Troubleshooting -999 Access denied

Ensure the ActionWorker Account has proper privileges on the client, WMI service is running and the Firewall allows WMI(in).

BitTruster leverages WMI to manage BitLocker and TPM and on the client computer. In order to do that the BitTruster ActionWorker Service needs to have administrative privileges on the client computers. Typically, the ActionWorker Service runs with the same user that has been used during the installation of BitTruster. However, this can also be done with a dedicated Service Account that can be created for BitTruster purposes only. This account needs to be added to the ActionWorker Service and to the local Administrators group on the clients or any other group that has local administrator privileges on the client.

Error 999 could mean that it's either a permission issue, i.e. the ActionQueueWorkerService does not have admin permissions on this particular client or the WMI service is not running on the client or WMI is corrupt (you can run "winmgmt /verifyrepository" on the client to check this).

In most cases, it's an issue with the permissions that a user/group has been removed from the local Admin group on the client or is not part of the group anymore. It could also be a firewall issue but this is most likely with other firewall vendors than Microsoft.

[See also Troubleshooting -2147023174 RPC Client not available](#)

- Please check the service account that runs the ActionWorker Service on the BitTruster Server
- Please verify that this user has administrative privileges on the client computer that is showing this error.
- Please verify if the password of the service account has not been changed or expired.

If none of the above helped to solve the problem, please contact us via BitTruster Support, support@bittruster.com