WORKSHARE PROTECT SERVER 3.2

TROUBLESHOOTING GUIDE

Workshare

Version 2.0 | March 2015

Workshare Protect Server 3.2 Troubleshooting Guide

Workshare Ltd. (UK)
20 Fashion Street
London
E1 6PX
UK

Workshare Inc. (USA)
625 Market Street, 15th Floor
San Francisco
CA 94105
USA

Workshare Website: www.workshare.com

Trademarks

Trademarked names may appear throughout this guide. Instead of listing these here or inserting numerous trademark symbols, Workshare wishes to state categorically that no infringement of intellectual or other copyright is intended and that trademarks are used only for editorial purposes.

Disclaimers

The authors/publishers of this guide and any associated Help material have used their best efforts to ensure accuracy and effectiveness. Due to the continuing nature of software development, it may be necessary to distribute updated Help from time to time. The authors would like to assure users of their continued best efforts in supplying the most effective Help material possible.

The authors/publishers, however, make no warranty of any kind, expressed or implied, with regard to Workshare programs or Help material associated with them, including this guide. The authors/publishers shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the programs or associated Help instructions.

Copyright

TABLE OF CONTENTS

WHAT IS THIS DOCUMENT?

This document covers basic troubleshooting steps you can take when you have Workshare Protect Server 3.2 with the Routing Agent installed.

You can find more information about installing and configuring Protect Server and the Routing Agent from these guides on our knowledge base (http://workshare.force.com/knowledgebase):

- Workshare Protect Server 3.2 Admin Guide
- Workshare Protect Server 3.2 Routing Agent Admin Guide

If you require further assistance, contact Workshare Support.

UNDERSTANDING THE PROTECT SERVER WORKFLOW

When you have Workshare Protect Server with the Workshare Protect Server Routing Agent installed, mail is routed from Microsoft Exchange to Workshare Protect Server if it contains:

- One or more attachments; **and**
- One or more external recipients.

Workshare Protect Server sends the processed mail back to Microsoft Exchange Server, then Microsoft Exchange Server does the final mail routing, similar to the typical Microsoft Exchange Server setup of in the figure below.

This custom routing is performed by the Workshare Protect Routing Agent (a transport agent) on Microsoft Exchange Server. The configuration prevents a mail loop by ensuring that mail coming back from Workshare Protect Server does not get re-routed back to Workshare Protect Server.

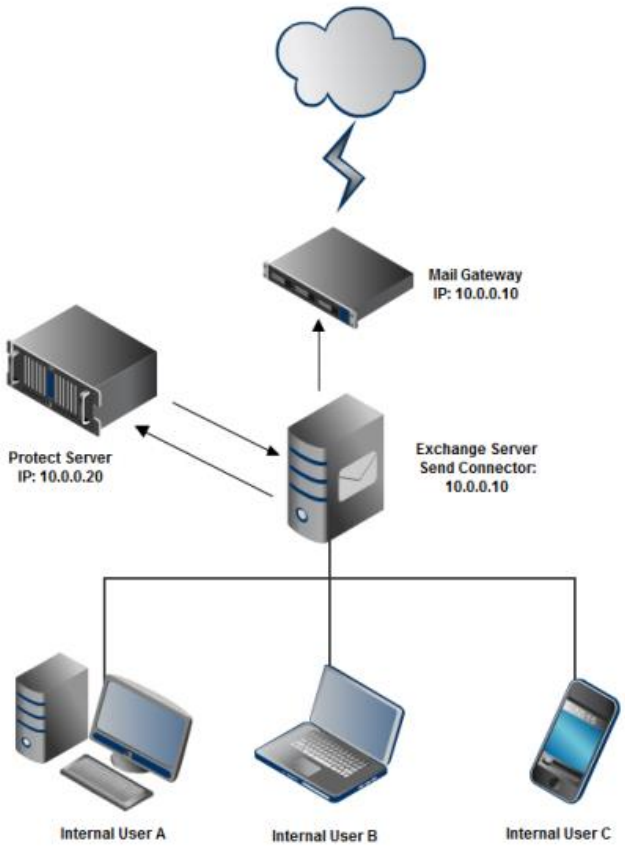


Figure 1: *What happens to an email once it has been delivered by a corporate mail server to Workshare Protect Server.*

The precise mail flow for Workshare Protect Routing Agent is as follows:

1. Mail sent by an internal user reaches the Microsoft Exchange hub transport server with the Workshare Protect Routing Agent installed.
2. Before Microsoft Exchange Server delivers the mail, it gets processed by the Workshare Protect Routing Agent. If the mail includes external recipients and one or more attachments, the transport agent will set routing on the mail to a special Send Connector, workshareprotectserver.com, that was created during the installation process and points

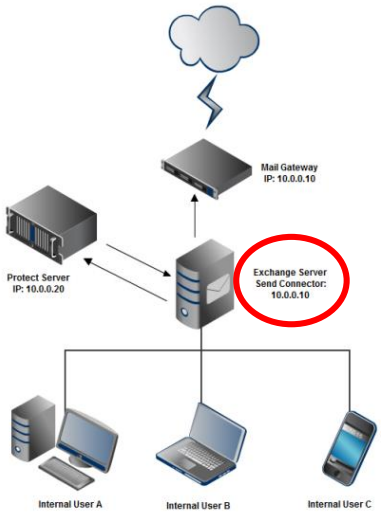
to Workshare Protect Server as its smart host. The transport agent also adds a MIME header to the mail to avoid a mail loop.

3. Workshare Protect Server will receive, inspect and possibly clean or convert the email attachment(s). It will then send the mail back to Microsoft Exchange Server. Workshare Protect Server will need to be configured to route all traffic back to Microsoft Exchange Server by setting its SMTP Server smart host to Microsoft Exchange Server on all domains in IIS 6 Manager.
4. Microsoft Exchange Server will receive the mail back from Workshare Protect Server. This is allowed by a Receive Connector created during installation. The Workshare Protect Routing Agent will see that the mail came from Workshare Protect Server and allow Microsoft Exchange to route the mail normally (to the mail gateway for external recipients and into the appropriate mailbox for internal recipients).

TROUBLESHOOTING MAIL FLOW ISSUES

1. Is Exchange receiving and sending mail?

The best way to confirm that Exchange is receiving and sending mail correctly is to look at the Queue Viewer on the Exchange Server and watch what happens when you send test emails. If you want to look for transmission errors that might have affected a particular message in the queue, right-click the message and select **Properties**.



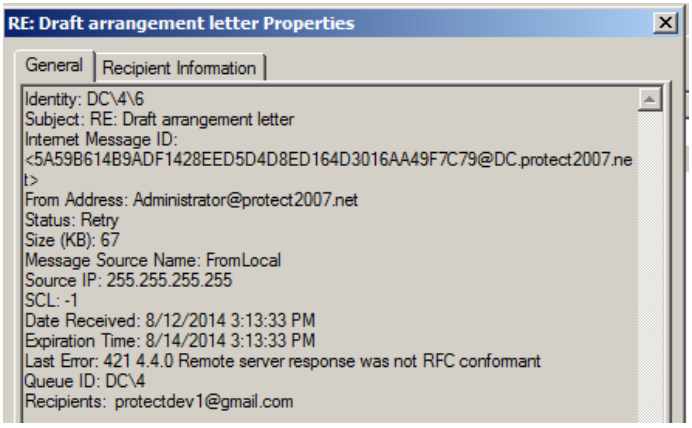
Follow these steps to view the Exchange queue:

1. Login to Exchange as the Exchange Admin.
2. Look at Exchange Management Console (EMC).
3. Launch the Queue Viewer from Toolbox.
4. If you're prompted to select a hub transport server, select one to test.
5. Send a test email and see what happens in the Queue Viewer.
    a. If the message count is not 0, emails are queued at Exchange because they can't be relayed to next mail server. Validate Exchange Send connectors in the Exchange Management Console:
        i. Ensure there is a custom Send connector routing mail through Protect Server as a smart host. This Send connector should have a lower cost than other Send connectors and the Address Space should be workshareprotectserver.com.
        ii. Ensure there is also be a second Send connector to forward mail to the final destination. The Address Space of this Send connector should be *, and it should either route mail to the next smart host or it should use DNS MX to route mail automatically.
        iii. Ensure the smart host authentication settings are correct. For Protect Server, smart host authentication should be set to None by default.
    b. If the message count is 0, there are two possible reasons why: 1) The mail flow could be working correctly and Exchange is sending the mail before it can be displayed in the queue viewer; or 2) Exchange hasn't received the mail. To confirm that mail is being received, look at the Exchange transport logs.

2. Does Protect Server have the ability to process mail?

Protect Server may be unable to process mail for a variety of reasons – for example, a Windows service that Protect Server depends on has crashed or Protect Server doesn't have a valid license. If Protect Server is unable to process mail, it will refuse the SMTP connection.

To confirm that Protect Server is refusing the SMTP connection, send a test email and look at Exchange to see how Protect Server responds. In the example below, the connection was refused because Protect Server didn't have a valid license. The screenshot shows what you would see by going to the Queue Viewer in Exchange and viewing the properties of one of the emails in the queue.



To understand why Protect Server is not processing email, go to the Protect Server web console and select the **Status** tab. Color-coded indicators show whether there are issues with the Protect Server mail flow. See **Appendix B: The Status Panel** for an in-depth explanation of how this tab works and what steps you can take if the indicators are yellow, grey, or red.

3. Is the SMTP Service on the Protect Server machine correctly receiving and sending mail?

Protect Server receives and sends mail using the IIS SMTP Service. When Protect Server receives mail, **smtpsvc** stores it in **C:\inetpub\mailroot\Queue**. The contents of this directory will fluctuate but trend towards empty as mail is received, processed, and sent.

To confirm whether the SMTP Service is receiving mail, go to **C:\inetpub\mailroot\Queue:**

a. If the directory is empty, confirm emails are being received by looking at the IIS SMTP logs (see **Appendix C: Logs**). If they aren't being received, review the IIS SMTP service settings (go to the knowledge base and see the **Workshare Protect Server Administrator's Guide**). If emails aren't being received and the service settings are correct, restart both IIS and the SMTP Service by opening the Command Prompt and entering these lines:

```
C:\> iisreset

C:\> net stop smtpsvc

C:\> net start smtpsvc
```

b. If the directory is not empty, emails aren't leaving Protect Server. Review the SMTP logs, checking the sc-status and sc-win32-status fields for SMTP error codes (typically 4xx, 5xx – see Appendix C: Logs). To confirm that Protect Server has the ability to send emails through the next email server, check that Exchange has a Receive connector that accepts connections from the Protect Server machine.

4. Is Protect Server processing mail correctly?

To confirm if mail is being processed correctly, review the Workshare MTA logs (see **Appendix C: Logs**). There is an issue with mail processing if:

- The logs are empty or are not being updated.
- The logs contain exception errors.
- There are error events reported in Windows Application event logs.

If you see an issue in the logs and you are unsure of how to proceed, contact Workshare Support.

If the logs don't show anything unusual, check whether the reason a specific email isn't being processed is that Protect Server has been instructed to bounce it. To confirm that Protect Server is bouncing mail:

1. Go to the Protect Server Web Console.
2. Navigate to the **Settings** tab.
3. Navigate to the **Bounce** page.
4. In the Protect Server settings, deselect the **Bounce** checkbox.
5. Send a test email to see if the issue persists.

If you do have a rule set to bounce emails, also ensure that an **Alert** email address is set. If this address has not been set, Protect Server will bounce the email but cannot notify the sender that their email has bounced. To check the **Alert** address:

1. Go to the Protect Server Web Console.
2. Navigate to the **Settings** tab.
3. Navigate to the **Alerts** page.
4. Ensure there is an **Alert** address.
5. Send a test email to see if the issue persists.

TROUBLESHOOTING ISSUES WITH A SPECIFIC EMAIL THAT HAS ARRIVED AT PROTECT SERVER

1. Determine how Protect Server processed a specific email

The **Messages** tab on the Protect Server web console can be used to determine if and how an email has been processed by Protect Server.

You can search for and filter messages by:

- **Date**
- **Email Address** (search with quotation marks, e.g. “myaddress@mycompany.com”)
- **Message ID** (search with quotation marks, e.g. “5A59B614B9ADF1428EED5D4D8ED164D3016B7D491E8A@DC.protect2007.net”)
- **Message Subject** (search with quotation marks, e.g. “Re: Term Review”)

To see the details of an email, click its **Subject**.

If an error has occurred, the log in **wps_mta** will contain diagnostic information (see **Appendix C: Logs**).

2. Badmail

The Badmail folder contains the emails that the SMTP service can’t deliver. Badmail messages for Protect Server are stored in **C:\inetpub\mailroot\Badmail**. You can monitor bad mail using the **Status** tab of the Protect Server web console (see **Appendix B: The Status Panel**).

There are several reasons why a message may be classified as bad mail, including:

- Bad pickup file (.EML file not in correct format)
- No recipient for email
- The email has been relayed too many times (potential loop detected)
- Unable to relay email

In each case, the procedure is as follows:

a. Examine the .BAD file in notepad to determine its origin. If the .BAD mail is a non-delivery report, examine its contents to determine the potential cause.
b. If the origin is external to organization, check IIS relay settings and ensure that Protect Server is not an open relay.
c. If the origin is internal, check that the email has not been relayed too many times by looking at the received header of an email to see which servers have received the message. Ensure there is no email loop.
d. Cross reference with **IIS SMTP** logs and **wps_mta** logs (see **Appendix C: Logs**) to determine the potential cause.

If no cause can be determined:

- If the origin is internal, check that the email has not been relayed too many times by looking at the servers who have received the email. Ensure there is no email loop.
- Attempt redelivery as relay issues may be intermittent:
    1. Rename .BAD files to .EML.
    2. Copy the files.
    3. Paste them in the pickup folder: **C:\inetpub\mailroot\Badmail.**

APPENDIX A. ROUTING AROUND PROTECT SERVER

If you require some time to debug an issue with Protect Server, you may want to temporarily remove Protect Server from mail infrastructure to ensure that mail delivery continues.

To remove Protect Server, disable the routing agent and the Workshare Send connector:

1. Open the Exchange Powershell Console.
2. Run the following commands:

```
Disable-TransportAgent "Workshare Protect Routing Agent"

Set-SendConnector "Workshare Protect Send Connector" -enabled
$false

Restart-Service MSExchangeTransport
```

To deliver the mail currently queued on Protect Server, you can manually move it to Exchange. **Any mail delivered this way will remain unprocessed by Protect Server**:

1. Go to the locations on Protect Server containing unprocessed .EML files:

   C:\inetpub\mailroot\Queue*.eml
   C:\inetpub\mailroot\Pickup*.eml

2. Copy the **.EML** files and paste them in Exchange's Pickup location:

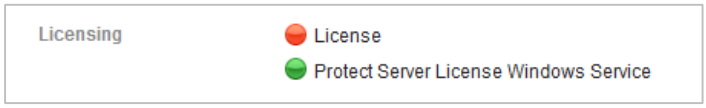
   C:\Program Files\Microsoft\Exchange Server\TransportRoles\Pickup

   The Pickup location is polled and processed every 5 seconds. Once processed by Exchange, the .EML file will be removed from this location so it can be delivered.

APPENDIX B. THE STATUS PANEL

The **Status** tab on the Protect Server web console is used to monitor whether Protect Server is processing mail. Indicators are used as follows:

- **Green:** Item is processing mail without issue. No action is needed.
- **Yellow:** A warning that the item is not working as expected, but it's not causing mail refusal. No immediate action is needed, but you should periodically check the status panel to ensure it has not turned red.
- **Red:** An issue with the item is causing mail refusal. The tables below explain what steps you should take if any item is red.
- **Grey:** Workshare is waiting for information about the item to be returned, so no information about the status can be provided. If the item is grey, wait for the color to change. If you have been waiting longer than two minutes, restart the service.



The tables below explain what steps you should take if any item is red. To find out more information about what's happening with any of these items, check the item's logs (see **Appendix C: Logs**).

Mail server

Item	Description	Steps to take if it's red

SMTP Queue Directory	Number of items that **smtpsvc** reports are in the queue.	• Restart the service:
		`iisreset`
		`restart-service smtpsvc`
		• Confirm upstream connectivity.

Badmailed Messages (Bad Pickup File)	Number of malformed pickup messages sent to the Badmail folder.	• Investigate as per Badmail section. • Delete Badmail items.
Badmailed Messages (General Failure)	Number of messages sent to the Badmail folder for reasons **other** than one of the following: • Hop count exceeded. • Delivery status notification could not be delivered. • Message contained no recipients.	
Badmailed Messages (Hop Count Exceeded)	Number of messages sent to the Badmail folder because they exceeded the maximum hop count.	

Item	Description	Steps to take if it's red
Badmailed Messages (NDR of DSN)	Number of Delivery Status Notifications sent to the Badmail folder because they could not be delivered. If a message is undeliverable, it is returned to the sender with a non-delivery report (NDR).	
Badmailed Messages (No Recipients)	Number of messages that could not be sent because there were no recipients.	

Remote Queue Length	Number of outbound emails waiting to be delivered.	• Restart the service:
		`iisreset`
		`restart-service smtpsvc`
		• Confirm upstream connectivity.

Remote Retry Queue Length	Number of outbound emails to retry.	
Event Message Queue	MSMQ queue for email processing results.	This item will go red if the message queue cannot be accessed. If this happens, the status message will advise what to do.
SMTP Sinks	Displays whether Protect Server is attached to IIS SMTP Server events.	Reinstall Protect Server.

Simple Mail Transfer Protocol (SMTP) Windows Service	Confirms the SMTP Service is running.	Restart the service:
		`iisreset`
		`restart-service smtpsvc`

Free Diskspace (System Temp)	Amount of space available for Protect Server mail processing.	n/a
Free Diskspace (Queue)	Amount of space available on the IIS queue directory.	This item will go red when there's less than 1GB of free space. The item never goes yellow.
Free Diskspace (Pickup)	Amount of space available on the IIS pickup directory.	This item will go red when there's less than 1GB of free space. The item never goes yellow.
tFree Diskspace (Drop)	Amount of space available on the IIS drop directory.	n/a

Licensing

Item	Description	Steps to take if it's red
License	Confirms the Protect Server is valid.	Purchase a valid license.
Protect Server License Windows Service	Confirms the Workshare Protect Server License Service is running.	Restart the service: `restart-service WPSLicenseService`

Auditing

Item	Description	Steps to take if it's red
Database	Confirms connectivity with database.	• Ensure database server is running and that the **ProcessorRole user** is assigned in the **ProcessorRole**. • Check **RemoteDatabase ConnectionString** in `%programdata%\Workshare\Protect Server\<version>\Configuration\db.config` • Check audit service is running as the ProcessorRole user, and that the correct password is set.
Event Message Queue Size	Number of email processing results pending storage in database.	
Event Message Queue	Name of the MSMQ queue for email processing results pending storage in database.	If this item goes red, the status message will advise what to do.
Protect Server Audit Windows Service	Confirms the Workshare Protect Server Audit Service is running.	Restart the service: `restart-service WPSAuditService`
Message Queuing Windows Service	Confirms the Message Queuing Service is running.	Restart the service: `restart-service MSMQ`

Profile

Item	Description	Steps to take if it's red
Active Profiles	Number of active profiles.	n/a
Profiles Changed	Time when profiles were last changed in cache. The expected time is within one minute from when the profiles were changed.	If this item goes red, the status message will advise what to do.
Profiles Synchronization	Time when profile service last synchronized the local profile store against database.	n/a
Protect Server Profile Windows Service	Confirms the Workshare Protect Server Profile Service is running.	Restart the service: `restart-service WPSProfileService`

Mail updater

Item	Description	Steps to take if it's red
Mail Updater Message Queue	Name of the MSMQ queue for email processing results pending storage in database.	n/a
Mail Updater Message Queue Size	Number of messages pending update with Sent Items folders.	n/a
Rapid Retry Message Queue Size	Number of messages pending retry of update with Sent Items.	n/a
Mail Updater Retry Queue	MSMQ queue for email processing results pending storage in database.	n/a
Mail Updater Retry Queue Size	Number of messages pending retry of update with Sent Items.	n/a
Exchange Web Services Connectivity	Confirms connectivity to EWS.	Check that the settings in the Mail Updater are correct: • Is it connected to the right server? • Is the impersonator username/password correct? • Is the correct version for Exchange selected? If these are correct, then go to the Protect Server machine and from Internet Explorer, browse to the EWS URL you supplied. This will confirm whether Protect Server is able to talk to EWS or not. If you're unable to browse, check your firewall and EWS settings.
Protect Server Mail Updater Windows Service	Confirms the Workshare Protect Server Mail Updater Service is running.	Restart the service: `restart-service WPSMailUpdaterService`

Active Directory cache

Item	Description	Steps to take if it's red
Active Directory Cache	Confirms the Workshare Protect Server Active Directory Cache Service is running.	Restart the service: `restart-service WPSAdcacheService`

APPENDIX C. LOGS

Protect Server logs

Protect Server uses Microsoft Enterprise Logging Library. This is controlled by the logging.config file kept in **%programdata%\Workshare\Protect Server\<version>\Configuration\logging.config**.

The key settings are **logging severity** and **logging location**. By default, only errors are logged to the following locations:

Service	Log Location
Workshare Protect Server Active Directory Cache Service	%TEMP%\wps_adcache.log
Workshare Protect Server Audit Service	%TEMP%\wps_audit.log
Workshare Protect Server Health Service	%TEMP%\wps_health.log
Workshare Protect Server License Service	%TEMP%\wps_license.log
Workshare Protect Server Mail Updater Service	%TEMP%\wps_mailupdater.log
Workshare Protect Server Profile Service	%TEMP%\wps_profiles.log
Workshare Protect Mail Transport Agent	%TEMP%\wps_mta.log
Workshare Protect Server Dashboard	%TEMP%\wps_web.log

The location of **%TEMP%** will depend on which user the service runs as. By default, this is the Processor Role user (eg: **C:\Users\<User>.<Domain>\AppData\Local\Temp**). If the service is running as **LocalSystem**, the **%TEMP%** location is **C:\windows\temp**.

To change the logging location, make the following modification to the **logging.config** file:

1. Search for: **filename="%TEMP%**
2. Replace with: **filename="<new location>**

To change the logging severity, make the following modification to each File Trace Listener element:

Change:

```
filter="Error"
```

To:

```
filter="All"
```

This example shows a **logging.config** file, highlighting the areas to be modified:

```
<add

name="Health File Trace Listener"
type="Microsoft.Practices.EnterpriseLibrary.Logging.TraceListeners.Rolling
FlatFileTraceListener, Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.414.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"

listenerDataType="Microsoft.Practices.EnterpriseLibrary.Logging.Configurat
ion.RollingFlatFileTraceListenerData,
Microsoft.Practices.EnterpriseLibrary.Logging, Version=5.0.414.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35"

fileName="%TEMP%\wps_health.log"

footer=""

formatter="Text Formatter"
```

```
header=""
rollFileExistsBehavior="Increment"
rollInterval="Hour”
filter="Error" />
```

Protect Routing Agent logs

By default, Protect Routing Agent logs to Windows Event Application Logs (see “Protect Server” event source). However it can be configured to log to file:

1. In Notepad, open: **C:\Program Files\Workshare\Protect for Exchange\Workshare.ProtectServer.Exchange.dll.config”**
2. Change (line 65):

   ```
   <allEvents switchValue="Off" name="All Events">
   ```

   To:

   ```
   <allEvents switchValue="All" name="All Events">
   ```

3. Change (line 41):

   ```
   <add fileName="%TEMP%\ProtectServerExchangeVerbose.log"
   ```

   To:

   ```
   <add filename=”<New file location>"
   ```

The logs for the Protect Routing agent are written to **%Windir%\ServiceProfiles\NetworkService\AppData\Local\Temp\ProtectServerExchangeVerbose.log.**

IIS SMTP server logs

To set IIS SMTP Server Logs, on the Protect Server machine:

1. Right-click **[SMTP Virtual Server #1].**
2. Select **Properties.**
3. In **General tab**, ensure the "Enable logging" is selected.
4. Ensure **Active log** format is **W3C Extended Log File Format.**
5. Click **Properties.**
6. Set **Log file directory** to the location where you would like to store the logs.
7. In **Advanced**, ensure the following fields are ticked.
8. Make sure the following checkboxes are selected:
    - Date
    - Time
    - Client IP Address
    - User Name
    - Service Name
    - Server Name
    - Server IP Address
    - Server Port
    - Method
    - URI Query
    - Protocol Status
    - Protocol Substatus
    - Win32 Status
    - Bytes Sent
    - Bytes Received
    - Time taken