# REMOTE AGENT MODULE (RAM)

User Guide

GLOBALSCAPE

| GlobalSCAPE, Inc. (GSB) | |
|---|---|
| | Corporate Headquarters |
| **Address:** | 4500 Lockhill-Selma Road, Suite 150, San Antonio, TX (USA) 78249 |
| **Sales:** | (210) 308-8267 |
| **Sales (Toll Free):** | (800) 290-5054 |
| **Technical Support:** | (210) 366-3993 |
| Web Support: | http://www.globalscape.com/support/ |



*February 14, 2019*

# Table of Contents

## Introduction to Remote Agents

The Remote Agent Module (RAM) for EFT Enterprise provides centralized control for automating transactions from distributed systems. RAM enables automatic interactions between branch offices, point-of-sale terminals, business partners, field agent laptops, or other remote systems and your EFT server residing in a central location. Install the *Remote Agent* service at the remote location, then enable the agent to process files that arrive in a monitored "hot" folder, or retrieve or send files to EFT on a schedule. Remote Agents call home routinely to gather updated instructions, removing the need for administrators to deploy and manage automation scripts manually at each branch office or remote location. RAM provides much of the power of EFT Event Rules in a package that takes just a few megabytes of space and can be deployed in seconds.

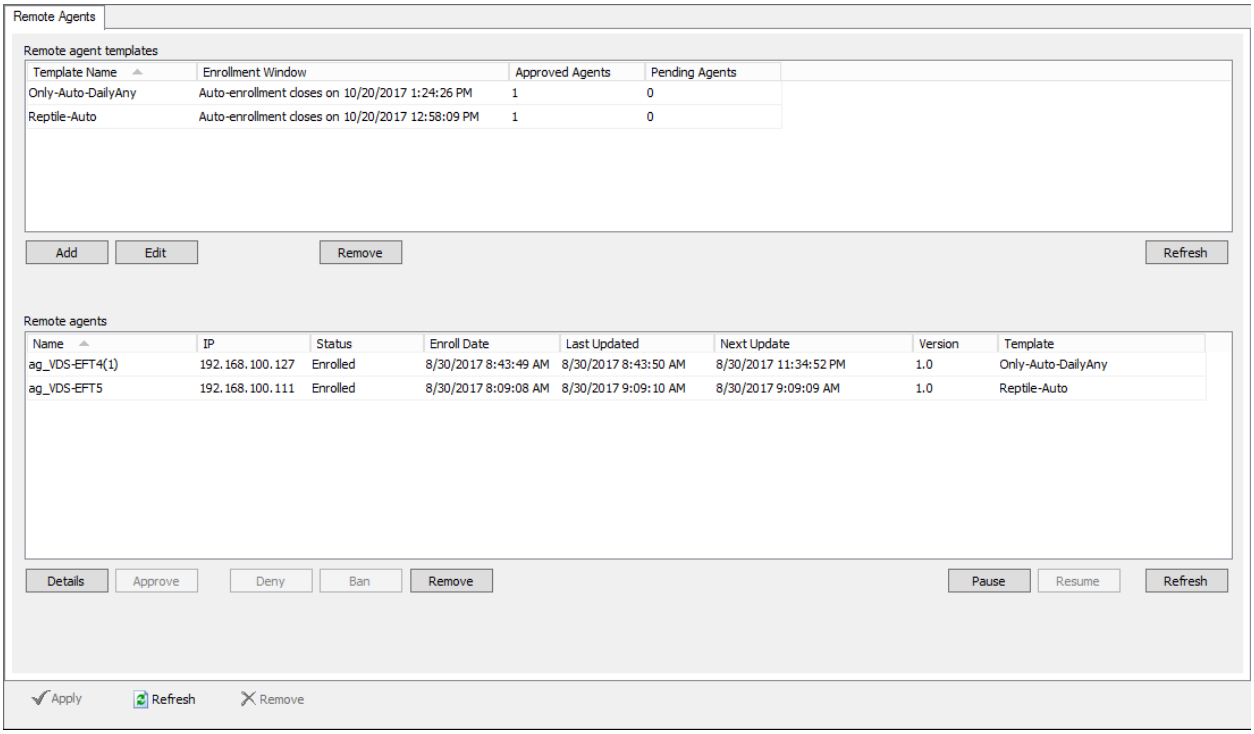
Remote Agents can be defined regardless of authentication method used on the Site, and leverages the Site's security settings, including transfer speed, and socket connection. Remote Agent connection is allowed only over HTTPS. RAM uses the system's default proxy settings (i.e., the configuration in Internet Explorer under Internet Options > Connections tab > LAN settings for proxy), which is used by all apps that require Internet access. For every connection, the Agent's and Site's banned IPs list and client SSL certificate is checked. EFT fails the authentication attempt if the certificates do not match.

*There are no administrator, user, or client connections at the Remote Agent end of the connection. The Remote Agent connection is "headless," meaning there is no interface.*

Each Remote Agent:

- Receives the initial rule set assigned to it, along with API key (GUID), certificates, etc.
- Calls home periodically to receive updated rule sets (i.e., gets new orders)
- Rules are triggered by EFT Timer and Folder Monitor logic; rules can push/pull files to the "home office" only

EFT displays interaction between end points and central hub, captures interaction of Remote Agents when requesting updated instructions, and allows administrators to easily add, modify, and remove Remote Agents and templates.




## Installing Remote Agents

The Remote Agents requirements include Visual C++ and Redistributable for Visual Studio 2010 and 2015 for installation. The Remote Agent module has been verified to work on the following operating systems: Windows Server 2016, Windows Server 2012 R2, Windows 10, Windows 8.1, and Windows 7.

*In EFT v7.4.5.6, RAM will not work on a Site that uses LDAP and CAC. Instead, create a separate GSAuth Site for RAM.*

The following installers are provided:

- **EFTRemoteAgentBundle.exe** is a bootstrapper package that contains the MSI, which verifies/installs the prerequisites and the application. You can run the EFTRemoteAgentBundle.exe and manually input the host, port, and template ID. The EXE file has an installer wizard in which you input the host, port, and Template ID. You can still use the EFTRemoteAgentBundle.exe if the prerequisites are installed.
- **EFTRemoteAgent.msi** does not contain the prerequisites. You would use this one if the prerequisites are already installed. The MSI is mainly used for System Center Configuration Manager (SCCM), group policy deployment, if you want a silent installation.

The administrator should make the EXE available to download via WTC or a shared Workspace. The URL, such as https://192.168.100.101/BOE/EFTRemoteAgentBundle.exe can be found in the Remote Agent Template. After logging in to the WTC, the EXE is downloaded.

The Remote Agent can be installed at command line using the default script in the folder in which you downloaded the EXE. Ensure that the EXE is in the same directory as you run the script.

```
EFTRemoteAgentBundle.exe /i acceptEula="yes" host="192.168.100.101" port=443
tid="075a9515-7861-4ecc-b56a-02d1e6c0cd25"
```

or

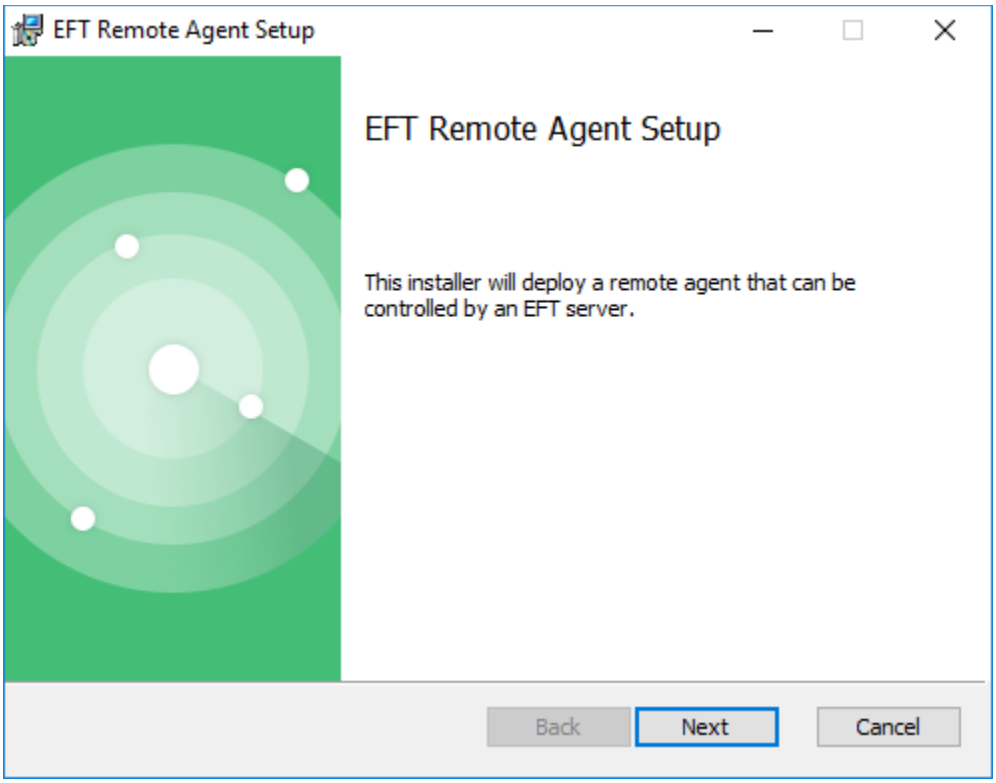
```
msiexec.exe /i EFTRemoteAgent.msi acceptEula="yes" host="192.168.100.101" port=443
tid="075a9515-7861-4ecc-b56a-02d1e6c0cd25" /qn
```

The benefit of running the script instead of launching the executable is that the host, port, and template ID (tid) fields are completed automatically. For manual installations, the EFT administrator will have to provide the EFT host address, port, and Template ID so that you can enter the information manually.

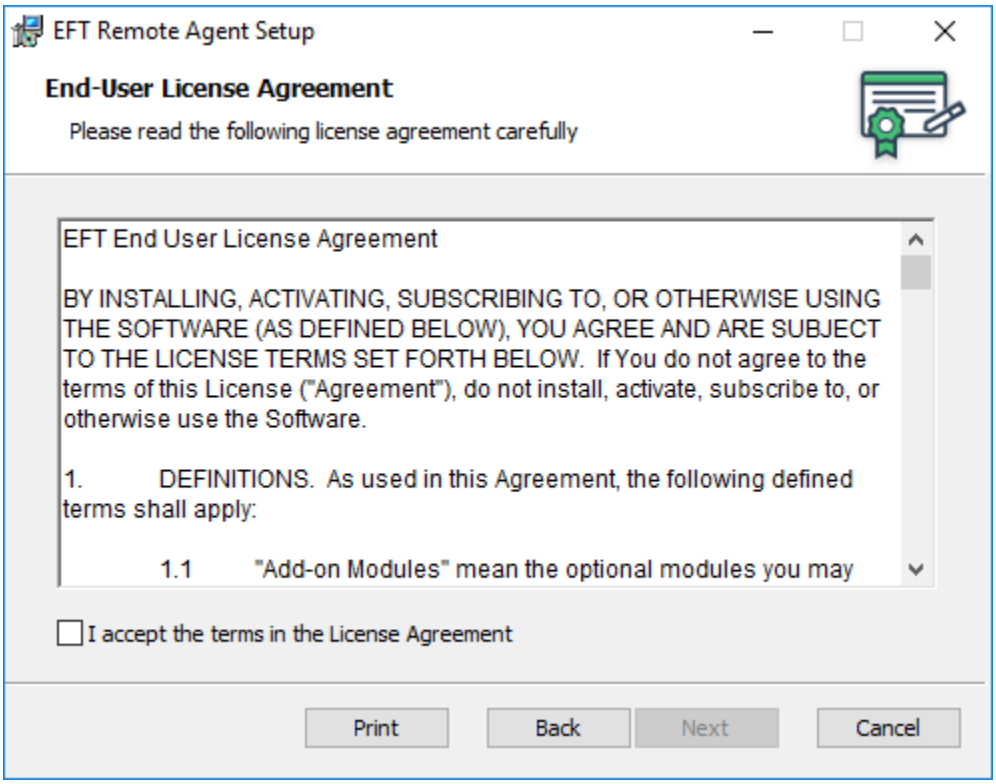
### To install the Remote Agent Bundle

1. On the computer on which the Remote Agent is to be installed, execute the installer. The **Remote Agent Bootstrapper** installer wizard appears.

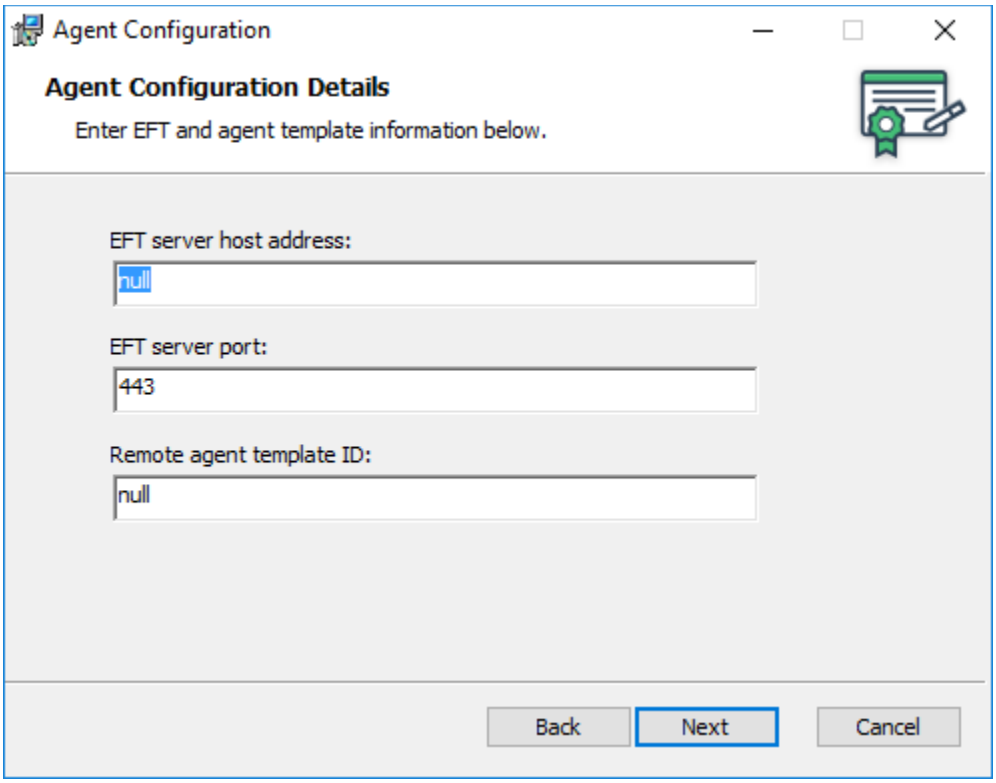

2. The bootstrapper checks for and installs prerequisites, if not already installed, then launches the Remote Agent installer wizard.
3. Click **Install**. The installer appears.



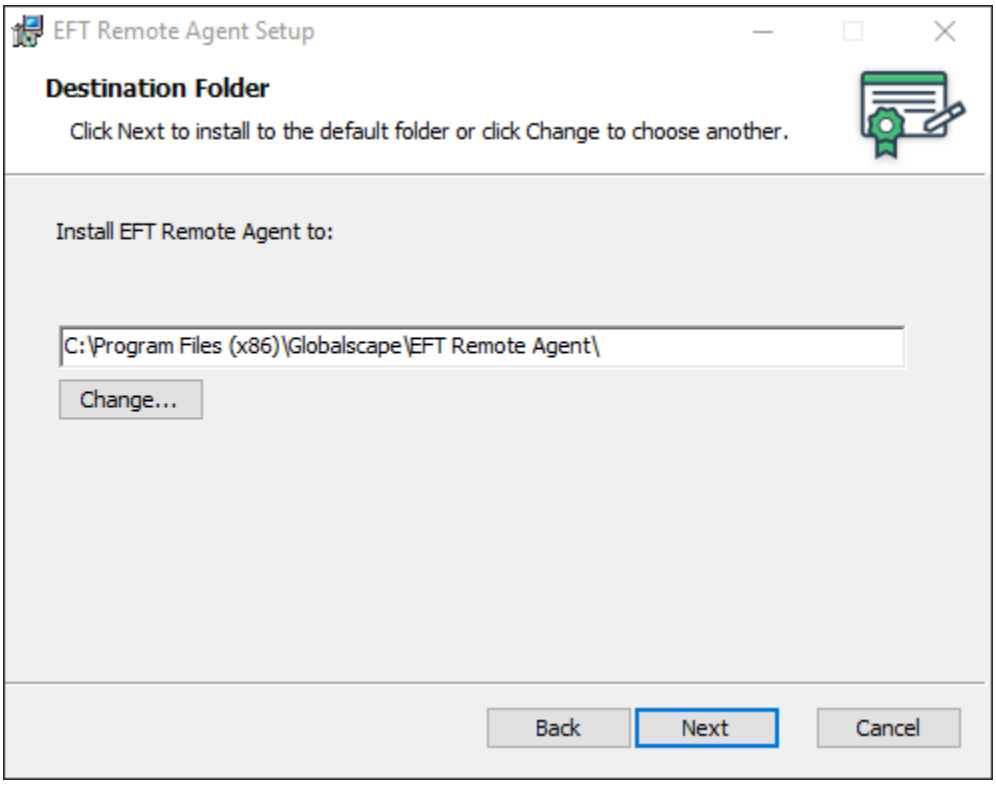

4. Click **Next**. The End-User License Agreement appears.



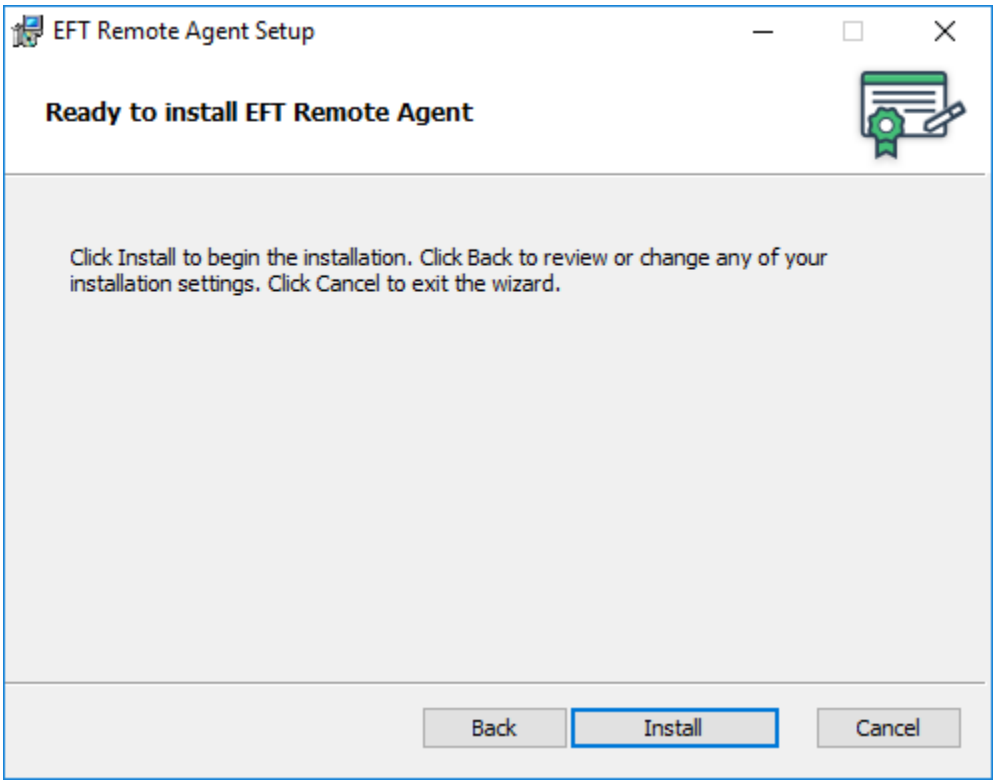

5. Select the check box, then click **Next**. The **Configuration** screen appears.



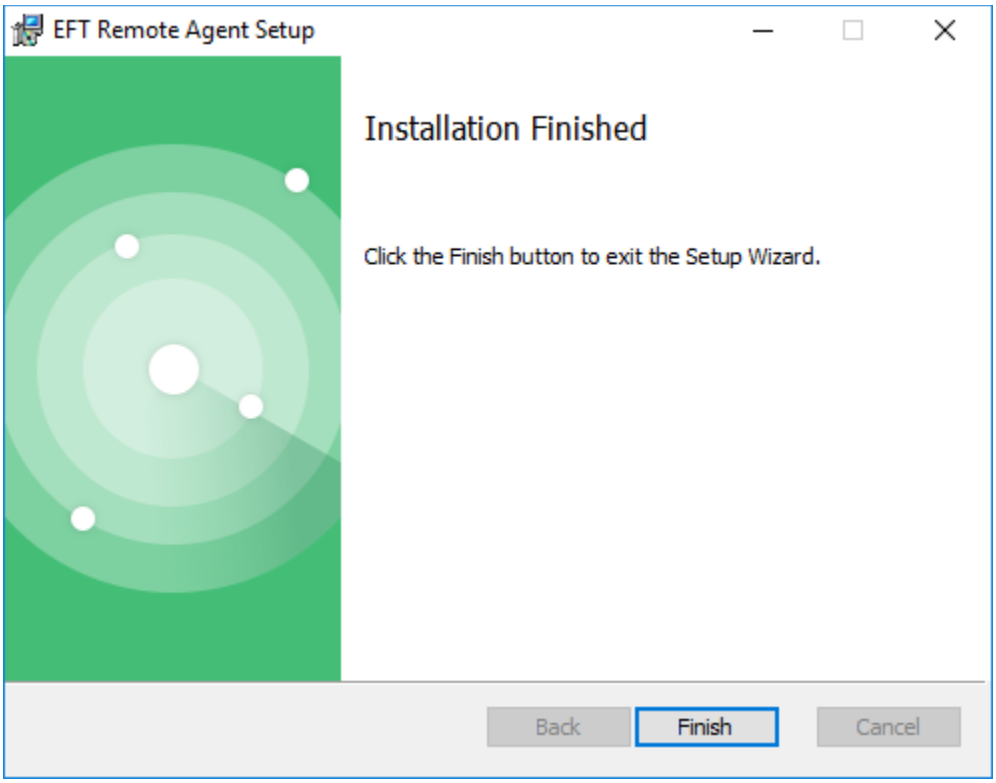

6. If you are running the installer manually (not from a script) you must provide the EFT server host address, EFT server port, and Remote agent template ID.
7. Click **Next**. The **Destination Folder** screen appears.



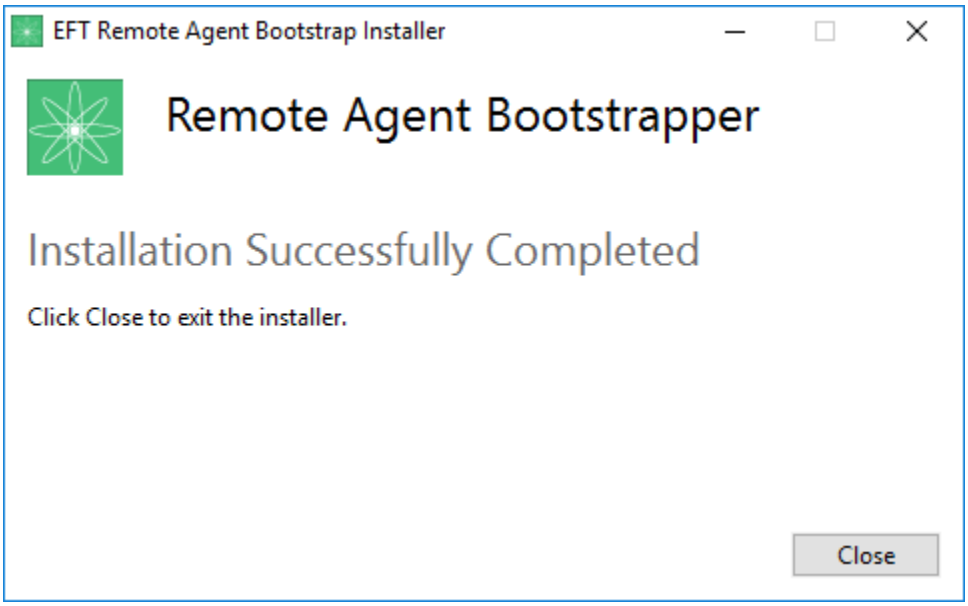
8. By default, the Remote Agent is installed in **C:\Program Files (x86)\Globalscape\EFT Remote Agent**. If you want to install in a different location, click **Change**.
9. Click **Next**. The **Ready to install** screen appears.




10. Click **Install**. The **Finished** screen appears.




11. Click **Finish**.




12. Click **Close** to exit the installer.

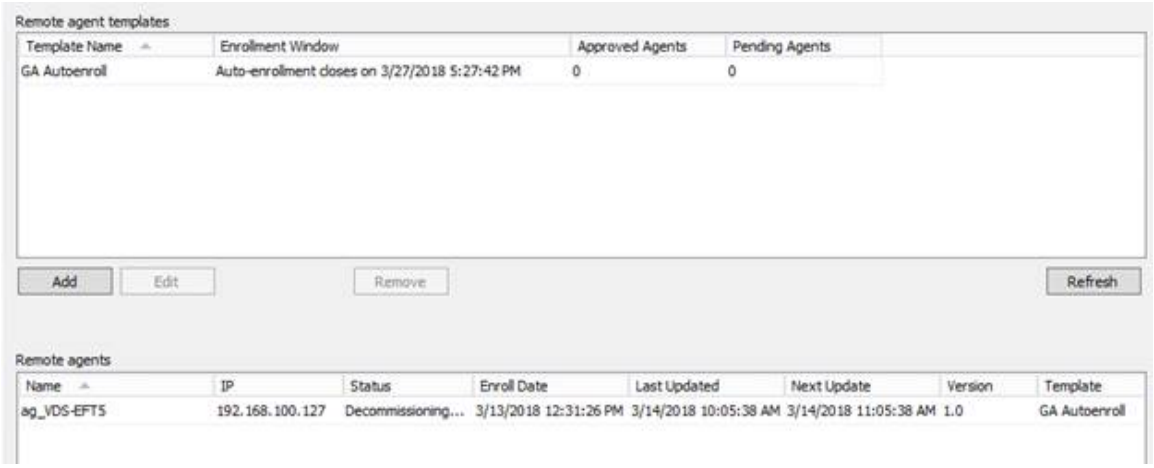
On the EFT computer, Remote Agents node, you will see the Remote Agent connect. If manual enrollment is specified, you will need to click the Remote Agent in the list, then click **Approve**. You may have to wait for the next update to see a change in status.

# Upgrading RAM

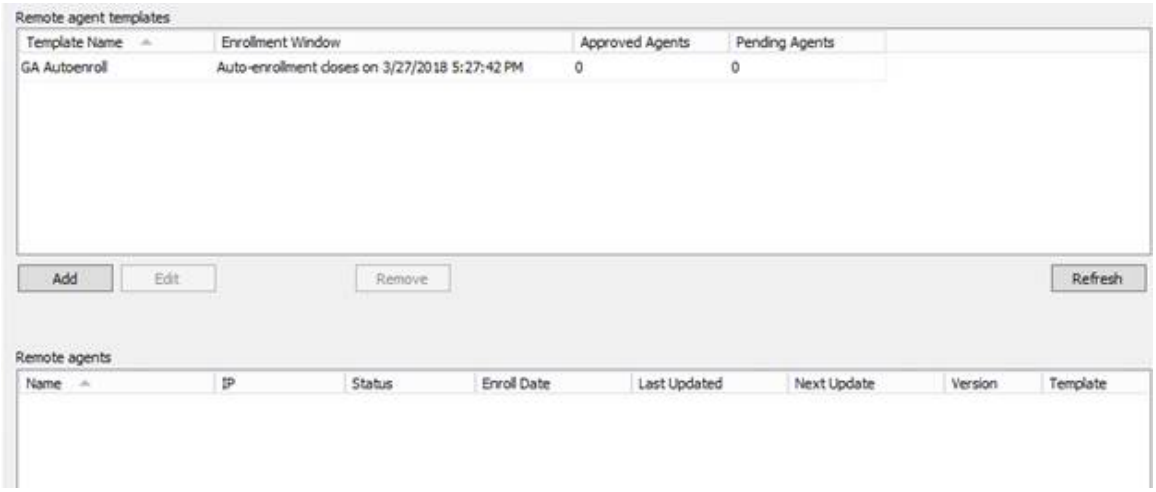
When you upgrade EFT, you will also have to upgrade any RAM agents.

## To upgrade RAM

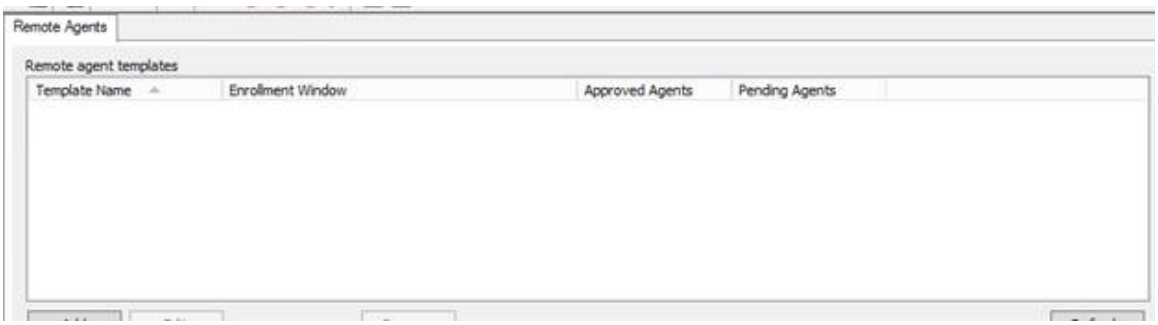
1. When upgrading RAM v1 to RAM v2, you must first decommission any Remote Agents you have defined on EFT.



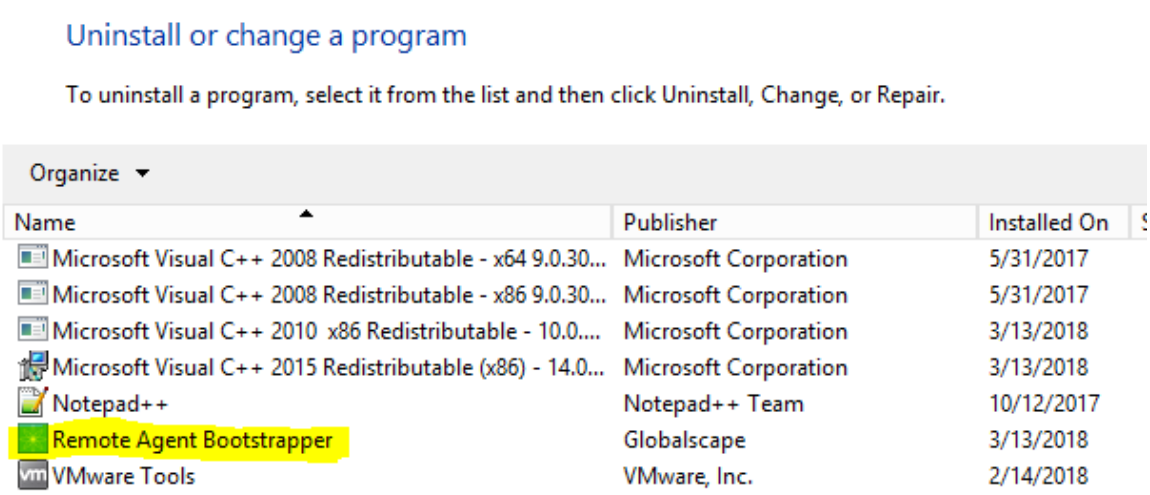

2. Verify agents have been decommissioned; they should no longer appear in **Remote agents** pane.




3. Remove any Agent Templates that appear in the **Remote agent template**s pane.

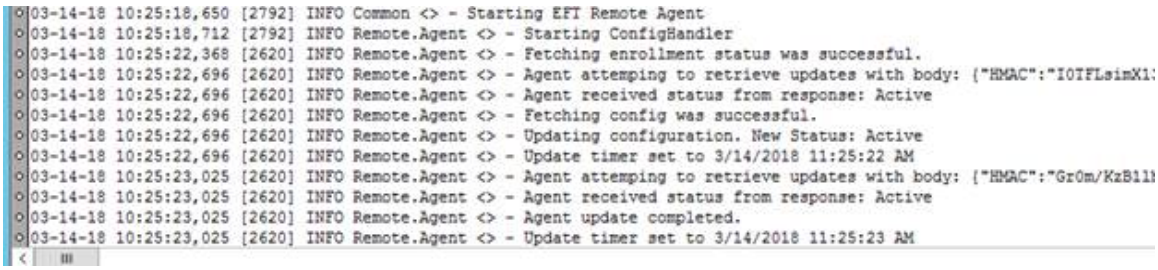


4. On the Remote Agent machine, uninstall **Remote Agent Bootstrapper**. (**Start > Settings > System > Apps & features**)

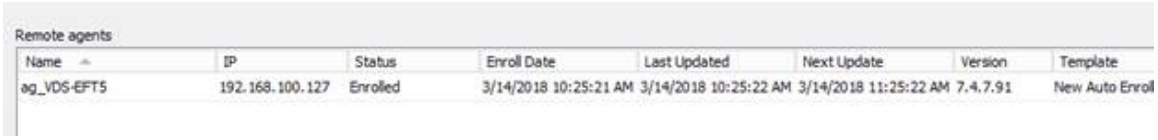



5. In (the newly upgraded) EFT, create a new Remote agent template.
6. In the **Remote Agent Template** dialog box, locate the new agent install URL script.
7. Install the Remote Agent(s).

   You should be able to see in the logs that it was updated.




8. The enrolled Remote agent enrolls itself, and then will appear in the **Remote agent** pane.




## Remote Agent Templates

In EFT, a Remote Agent template stores configuration and rules that can be shared by many Agents, and an installer script is generated for each Remote Agent template. Therefore, if one or more remote offices have one set of needs, and another set of remote offices has different needs, a separate remote agent template will distinguish between both sets of offices, allowing you to control each group separately.

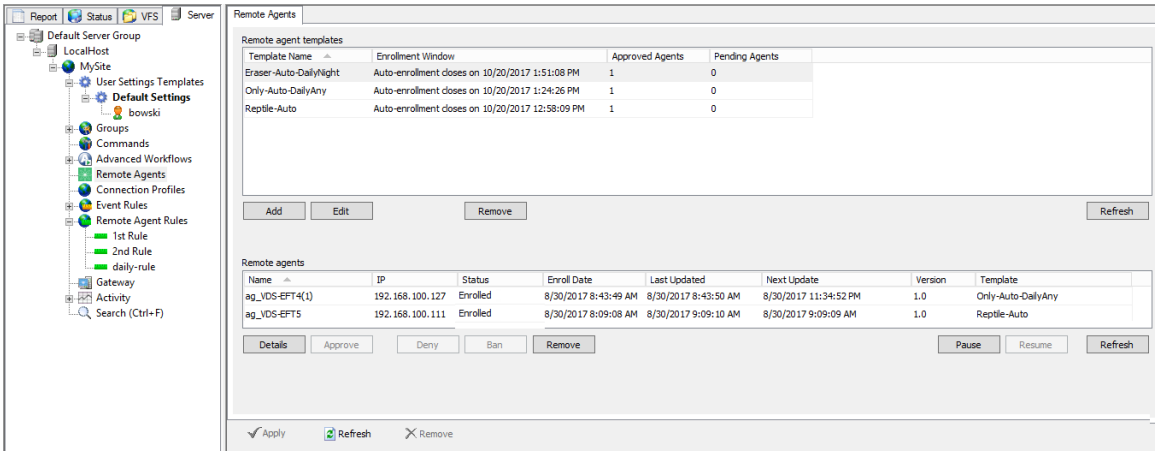
In addition to creating templates on this tab, you can monitor when Remote Agents have requested enrollment, are approved, denied, awaiting approval, or decommissioned, and information about the Remote Agents such as IP address, status, enrollment date, and dates when it was updated. The tab also provides options to deny, ban, or remove the agent, and pause and resume remote Agent rules.

Before creating your first Remote Agent Template, you should define a Remote Agent Event Rule. If you haven't created any Remote Agent Event Rules, you can still create the template, but then you'll have to edit the template after you create the Event Rule to add the Event Rule to the template.

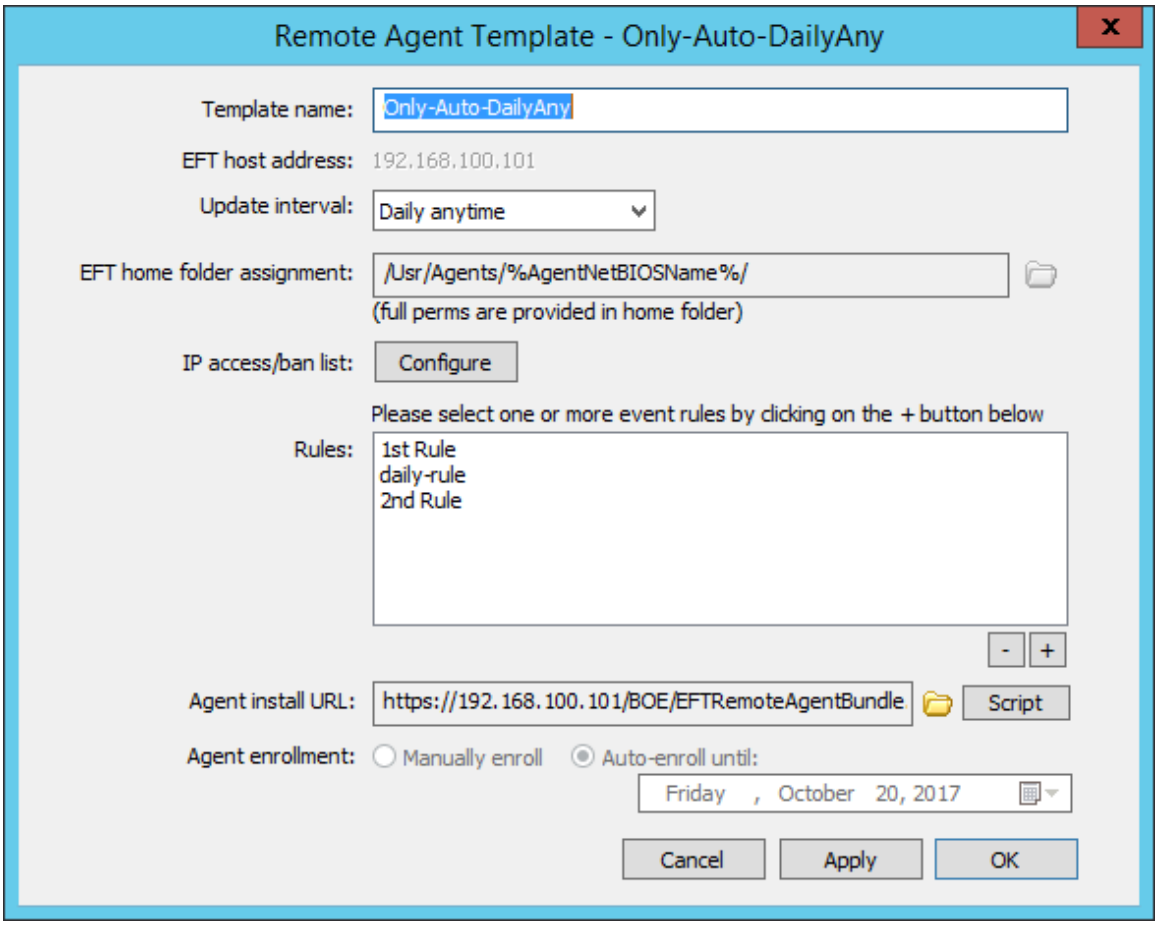
*Ensure that HTTPS is allowed on the port specified and that it is not being blocked by the Windows firewall at either end of the connection.*

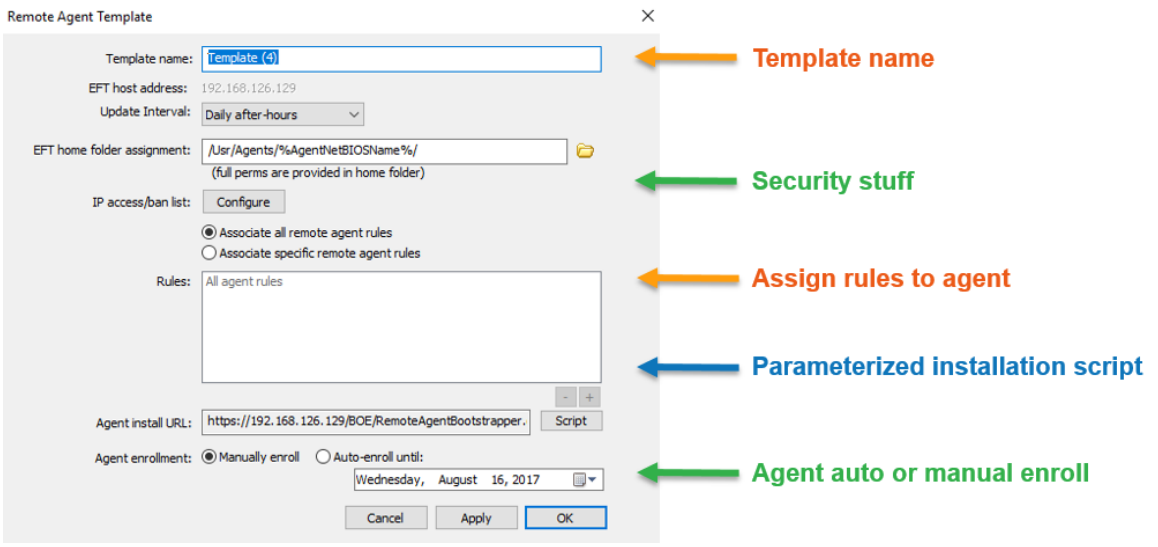
## To create a new Remote Agent template

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, expand the Site node, then click **Remote Agents**.



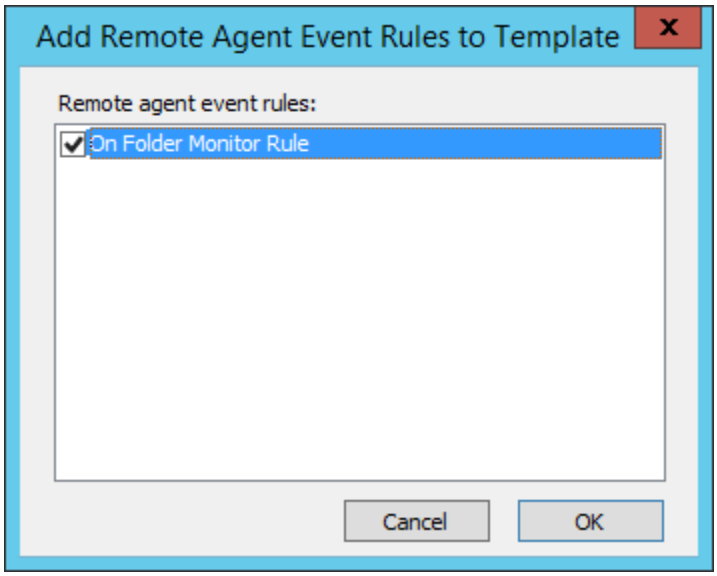

3. On the **Remote Agents** tab, click **Add**. The **Remote Agent Template** dialog box appears.




- **Template name** - The default name is Template with a number after it (which is incremented for duplicate names). If you expect to have only one template, the default name is probably fine. However, if you anticipate having more than one, you should give the templates descriptive names, such as "Western Region," "Los Angeles office," or "District 7." (Up to 130 characters.)

- **EFT host address** - Not editable in this dialog box
- **EFT server certificate** - Not editable in this dialog box
- **Remote agent cert** - Click **Configure** to create or choose an SSL certificate pair for administrator connections. Enrolled agents always verify validity, expiration, etc. of the server certificate provided against its local copy of the server's certificate that was assigned to the agent at enrollment. The Remote Agent fails the authentication attempt if the certificates don't match.
    - Agent logs the failure and failure reason
- **Update interval** - Specify when to contact EFT to check for and download updates. (Hourly, Daily anytime, Daily after-hours, Weekly, Weekly on weekends, Monthly)
- **EFT home folder assignment** - Agent's home folder in EFT
- **IP access/ban list** - Opens the **IP Access Rules** dialog box to view, add, edit, or remove IP addresses that are denied or allowed access to the Site.
- **Rules** - Click the PLUS SIGN to add Event Rules to this template.
  The **Add Remote Agent Event Rules to Template** dialog box appears. [Disabled rules will show as (Disabled)]



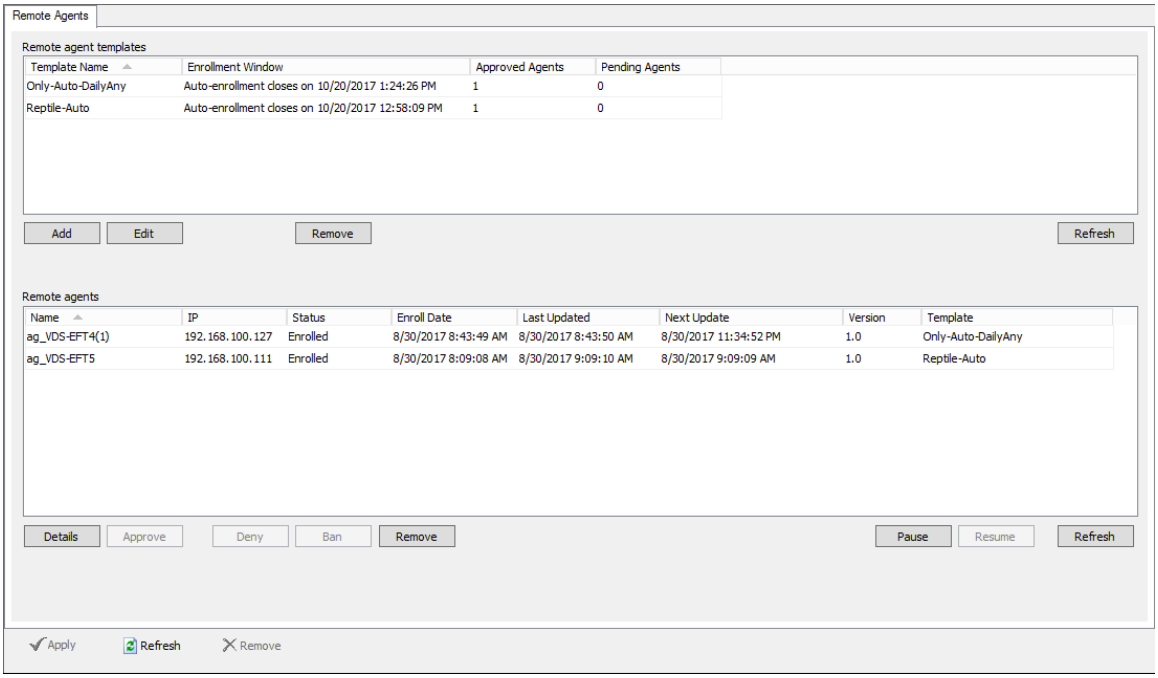

    - Click a Remote Agent Event Rule, then click **OK**.
- **Agent install URL** - The default path to install the EFTRemoteAgentBundle.exe appears in the box. By default, the script reads:

```
EFTRemoteAgentBundle.exe /i acceptEula="yes" host="localhost" port=443
tid="5d93bdfb-40a6-4f7e-b5da-8a67ac0d53f7"
```

Click **Script** to view the details. You should edit this to change the host and port number if you're not using "localhost" and port 443. (Port can be changed on the Site > Connections tab)

- **Agent enrollment** - Specify whether Remote Agents are manually or automatically enrolled:
  - **Auto enrollment** - If the Agent tries to install outside of the auto-enrollment windows the Agent will disable. A new template will have to be created and the Agent will have new template parameters. If **Auto-enroll** is chosen, the default expiration is 2 weeks from creation date.
  - **Manual enrollment** - If the Agent is approved on the EFT side but the Agent doesn't answer for 6 days due to network connection, turned off, etc., the service stops but stays enabled so that the next time the machine has connectivity it can enroll. ("Enrollment failure" appears in the **Status** column.)

4. Click **OK** to save the template. The template appears in the **Remote Agents** tab.




On the **Remote agents** tab, the following details are displayed:

- **Template name** - Displays the name of the Remote Agent template
- **Enrollment Window** - For automatic enrollment, this column indicates when the enrollment opportunity expires. Otherwise, it displays **Manual enrollment**.
- **Approved Agents** - Displays the number of Remote Agents that are using this template.
- **Pending Agents** - Displays the number of Remote Agents that have requested enrollment.
- **Name** - Remote agent name

- **IP** - Remote agent IP address
- **Status** - Enrolled, awaiting enrollment, decommissioning
- **Enrolled date** - Date/time when Remote agent was enrolled
- **Last updated** - Date/time of last Remote agent update
- **Next update** - Date/time when agent is scheduled to check for updates
- **RAM version number** - Version of RAM
- **Template name** - Name given when you defined the template

### Managing templates:

- **Add** - Click **to** create a new template
- **Edit** - Opens **the** Remote Agent Template dialog box so you can make changes. You cannot edit the following settings: host address, home folder assignment, and Agent enrollment period, (because doing so would cause the Remote Agent to fail).
- **Remove - Deletes a selected template.**
- **Refresh -** (top **pane**) Refreshes the list of approved and pending agents.

### Managing agents:

- **Approve** - Enables a Remote Agent that has requested enrollment
- **Ban** - Prevents **the** Remote Agent from requesting access
- **Deny** - Denies an enrollment or updates request
- **Details -** Refer to Managing Remote Agents.
- **Pause** - Pauses the Remote Agent Event Rules. The Remote Agent will still check for periodic updates on its defined update schedule.
- **Refresh** (bottom pane) - Refresh the list of agents to see updated status
- **Remove** - (bottom pane) Deletes the selected Remote Agent. Also know as decommissioning.
- **Resume** - Resumes the Remote Agent Event Rules to run at the next update interval.

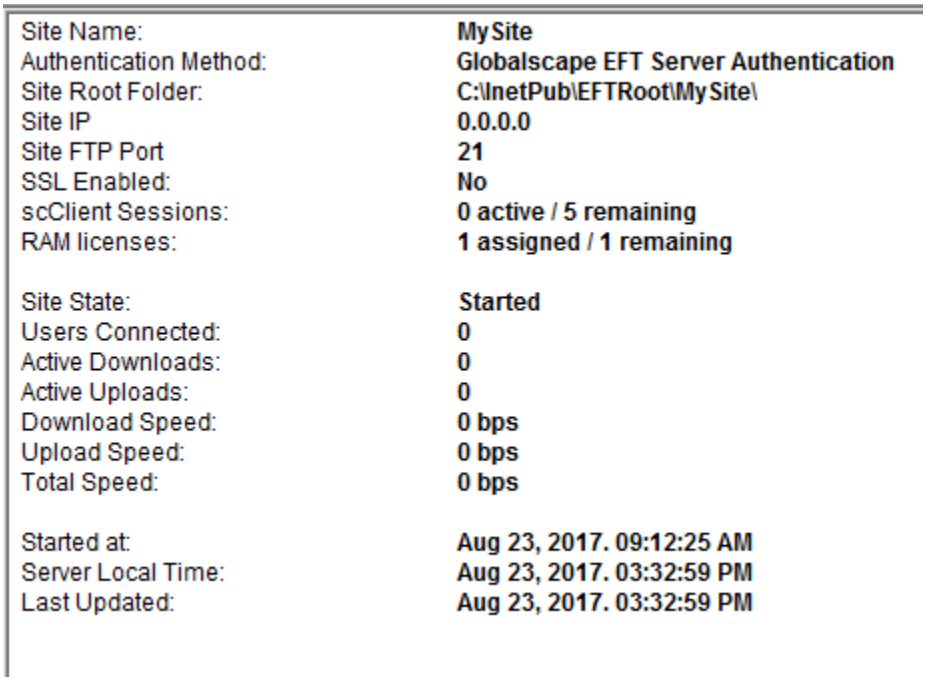
Refer to Managing Remote Agents for details of managing Remote Agents.

## Remote Agents License Status

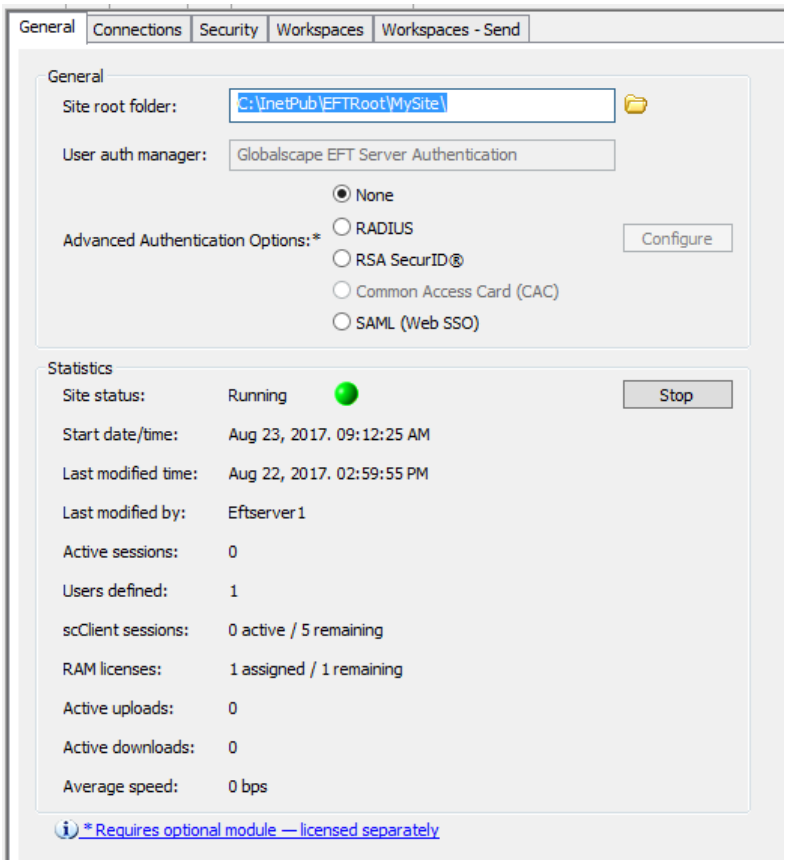
Each Remote Agent uses one Client Access License (CAL), whether the Agent is paused (disabled) or active. Removing an agent releases the CAL back to the pool of licenses available. New agents cannot be provisioned more than the number of CALs licensed. That is, if you have 5 Remote Agent CALs, you can only create 5 Remote Agents. In trial mode, you can only define one Remote Agent.

The Remote Agents license status can be viewed:

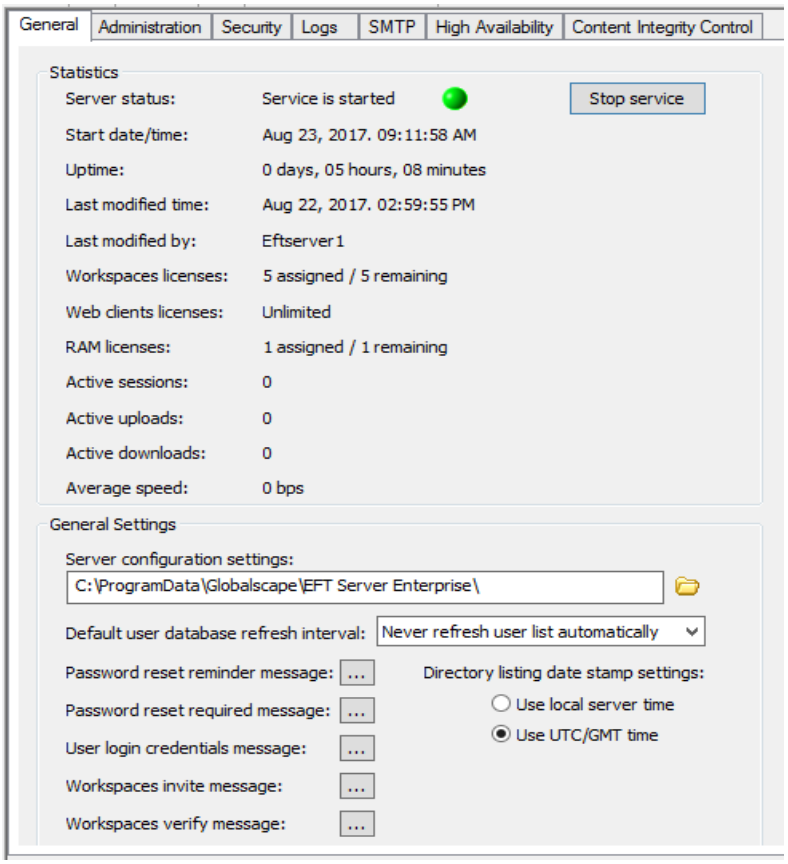
On the **Status** tab's **Site** node:



On the **Server** tab > **Site** node > **General** Tab:



And on the **Server** tab > **Server** node > **General** tab:




## Remote Agent Updates

Each Remote Agent receives the initial rule set assigned to it, along with API key (GUID), certificates, etc. from its assigned template. After the Remote Agent enrolls itself with EFT, it then calls home periodically to receive updated rule sets (i.e., gets new orders). This topic describes that process.

### Automatic Upgrades

- If the agent determines that the agent installer version (on disk) being advertised by EFT is different than its own version, the agent will download and run that installer (auto-upgrade)
- Agents will log their update process including any errors
- EFT will log from its perspective when it detects an agent update occurred, including any errors detected or provided by the agent
- EFT's installer will backup prior agent installers when performing a general (EFT) upgrade
- Agent update process only occurs for enrolled active or enrolled paused agents, but not pending enrollment or pending removal agents.
- Only agents that support auto-update will be able to update to a newer version. Agents installed prior to EFT v7.4.7 will not have this functionality.

- Failure to download the new agent installer will result in a logged failure and the agent will retry again on its next call home.
- After successfully downloading the new agent installer, if an agent fails to spawn the process to run the new installer, the agent will log and take itself offline.

### Enrolled remote agents will call home to obtain updated orders at agent service startup and at the defined update interval set obtained at enrollment for that agent template.

- Near real time - The Agent will check for updates every 15-30 seconds.
- Every 5 minutes - The Agent will check for updates every 5 minutes.
- Every 30 minutes - The Agent will check for updates every 30 minutes.
- Hourly - The Agent will check for updates every 60 minutes. The start timer is based on service start time (+60 minutes and repeat)
- Daily - The Agent will check for updates randomly  any time of the day and repeat daily at that same time
- Daily - afterhours - The Agent will check for updates randomly between 11PM and 6AM local time and repeat nightly at same the time.
- Time zones are with respect to the Agent's location
- For manual updates, "update now"

### If the Remote Agent fails to connect to EFT to receive updated instructions:

EFT allows a "grace period before failure" of one day for all update intervals. Below is an example of what happens when a failure occurs:

1. The agent logs a temporary update failure.
2. The agent tries again in 5 minutes, then 15 minutes, then 30 minutes. (These attempts will occur only for hourly and daily options.)
3. After 1 day of re-trying, the agent logs a failed update and then performs the specified option for update failure described below.
4. On the next scheduled update cycle, the agent will try to connect to EFT again.
5. If the agent service is restarted, the agent will repeat the connection process above.

### If an Agent fails to connect to EFT after repeated attempts in a 24-hour period, one of three actions can take place, as specified by the EFT administrator:

- Stop and disable the agent service and un-enroll the agent
- Stop and disable the agent service
- Stop the agent service only.

### If the agent is unable to connect after two entire update cycles, the agent will:

1. Log "critical failure to update."
2. Take itself offline (service stop)
3. Set its service to disabled.
4. Not reset itself to the pre-enrollment state.

### If the agent fails to authenticate when attempting to update its instructions (authentication or certification failure):

1. The agent will log the authentication failure(s)
2. The agent will try again in 5 minutes, then 15 minutes, then 30 minutes.
3. Once all retries are exhausted, the agent will log a failed update, then reset itself to pre-enrollment state. (Resetting itself provides an opportunity for admin to forcibly remove enrolled agents from EFT.)
4. The agent will agent will bring itself offline (service stop), as there is no point in trying again or to keep rules active if unable to authenticate.
5. The agent will set its service to disabled.
6. If the agent service is restarted, the enrollment process will occur again.

### If the agent successfully connected and authenticated:

1. The agent will communicate its agent version to EFT.
2. The agent will obtains its update interval, based on the agent's parent template.
3. The agent will obtain its designated list of rules associated with that agent, based on the agent's parent template
4. The agent and EFT will exchange when next call home will occur
5. The agent will obtain status information from EFT:
    - Whether agent should suspend (pause) its rules until further notification
    - Whether agent should re-activate (resume) its rules
6. EFT updates the last called home and next call home times in the agent list

### If the agent service is ever stopped (regardless of how/why),

- The ruleset and update interval is lost.
- When the agent service is started, it will call home and obtain updated orders.

When an agent is removed, that agent is unknown to EFT; all records of that agent's existence are removed. After a certain number of failed authentication attempts, the agent will essentially un-enroll itself and take itself offline.

## Remote Agent Rules

The **Remote Agent Rules** tab is where you can define automation rules that apply to the Remote Agents. The Remote Agent Event Rules trigger on the Remote Agents that you assign the rule to, not on EFT.

The Remote Agent Rules have limited triggers and Actions available, separate from EFT Event Rules:

- Event triggers for Remote Agents include Schedule (Timer) events, Folder Monitor events, and Folder Monitor Failed events.
- Event Actions for Remote Agents include Copy/Move action, Download action, and Stop processing this rule action.

Enrolled agents "call home" periodically to obtain their automation instructions, configurable in the Remote Agent template. If connection or authentication fails, the agent will perform retries as specified in the Remote Agent Event Rule configuration. If all connections/retries fail, then the Remote Agent Event Rule fails.

- Agents receive their rules on their update interval.
- Paused rules will take effect when the agent updates according to its update interval.
- Resumed rules will take effect when the agent updates according to its update interval.
- Remote agent rules can be created before or after template creation.

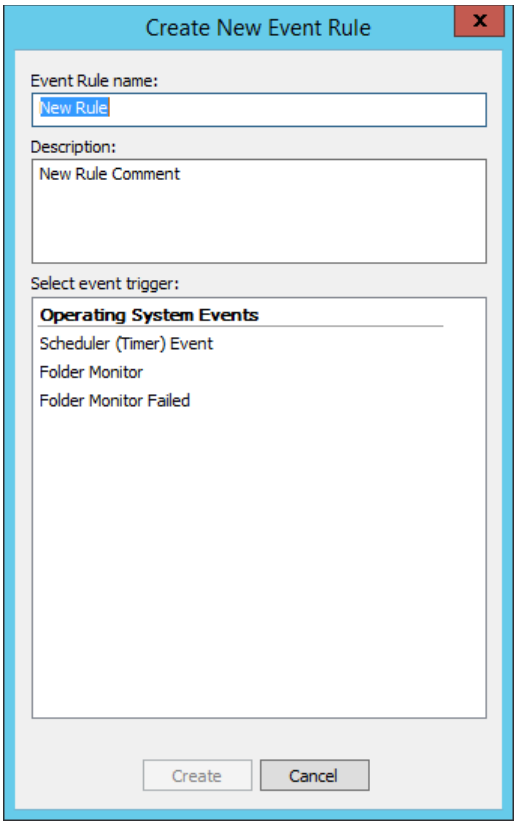
Automation instructions are configured within EFT Event Rules, allowing administrators to specify one or more “hot” folders the agent should monitor (relative to the agent’s file system), or a schedule, including complex recurring schedules, in which to initiate a transfer. Transfers can be uni- or bi-directional, meaning files can be uploaded from the agent or downloaded from EFT, depending on the desired outcome.

If an agent is properly enrolled, EFT will automatically authenticate the agent on connect, and authorize the agent to write to a designated home directory on the server. IT can optionally setup server-side Event Rules to then initiate automation sequences within EFT based on agents initiated transfers, thus completing the cycle of agent automation, agent transfer, central server receipt, and central server automation, such as integrating received files into a back-end system.

Keep in mind that their VFS folder is their home folder when defining Remote Agent Event Rules.

### To create a Remote Agent Rule

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, expand the Site node, then click **Remote Agent Event Rules**.
3. Next to the **Rules** pane, click **New**. The **Create New Event Rul**e dialog box appears.




4. Click an event trigger: Scheduler (Timer) Event, Folder Monitor, and Folder Monitor Failed.
5. Finish defining the rule, then click Apply.

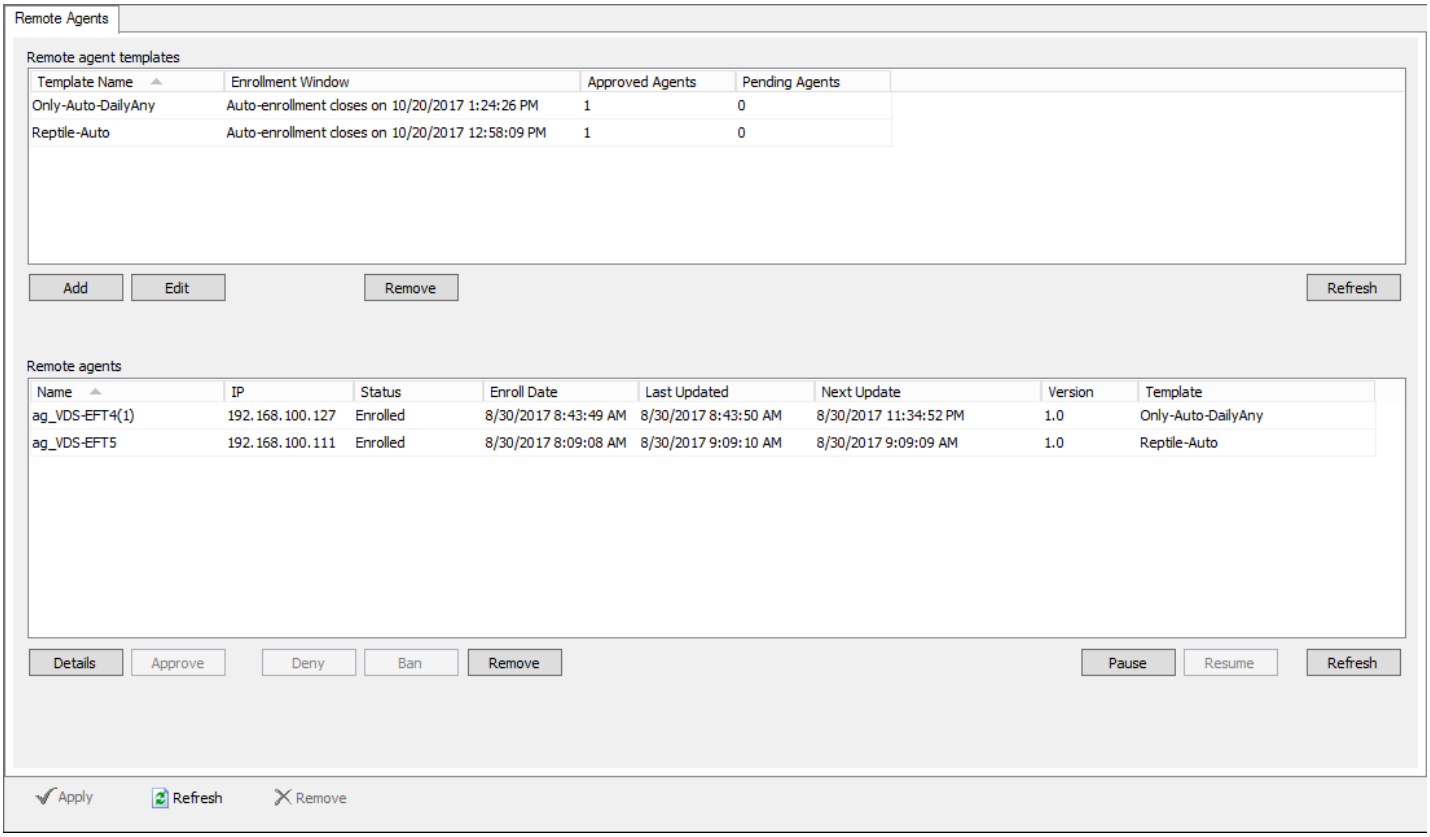
   The rule is now available for you to assign to Remote Agents in the Remote Agent template.

## Managing Remote Agents

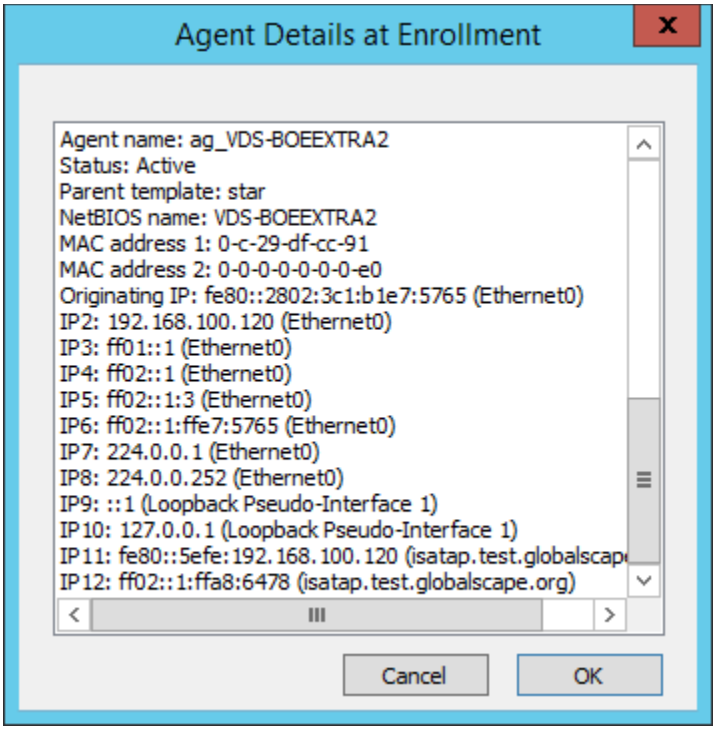
As Remote Agents request enrollment and updates, the Remote Agent's information appears in the bottom half of the **Remote Agents** tab of the Site.

### To manage Remote Agents

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, expand the **Site** node, then click **Remote Agents**.
3. In the bottom half of the **Remote Agents** tab, click the name of the Remote Agent that you want to manage.




- **Details** - Displays information about the Remote Agent: name, status, template, MAC addresses, IPs. Click **OK** to close the dialog box.




- **Approve** - Enables a Remote Agent that has requested enrollment

- **Deny** - Denies an enrollment or updates request
- **Ban** - Prevents the Remote Agent from requesting access
- **Remove** - Deletes the selected Remote Agent. Also know as decommissioning.
- **Pause** - Pauses the Remote Agent Event Rules. The Remote Agent will still check for periodic updates on its defined update schedule.
- **Resume** - Resumes the Remote Agent Event Rules to run at the next update interval.
- **Refresh** - Refreshes the list of approved and pending agents.

See also Remote Agent Templates.

## Remote Agent Context Variables

The Remote Agent Context Variables can be used in Event Rules. Each of the variables is described below. For more information about using context variables in EFT, refer to EFT Context Variables (List).

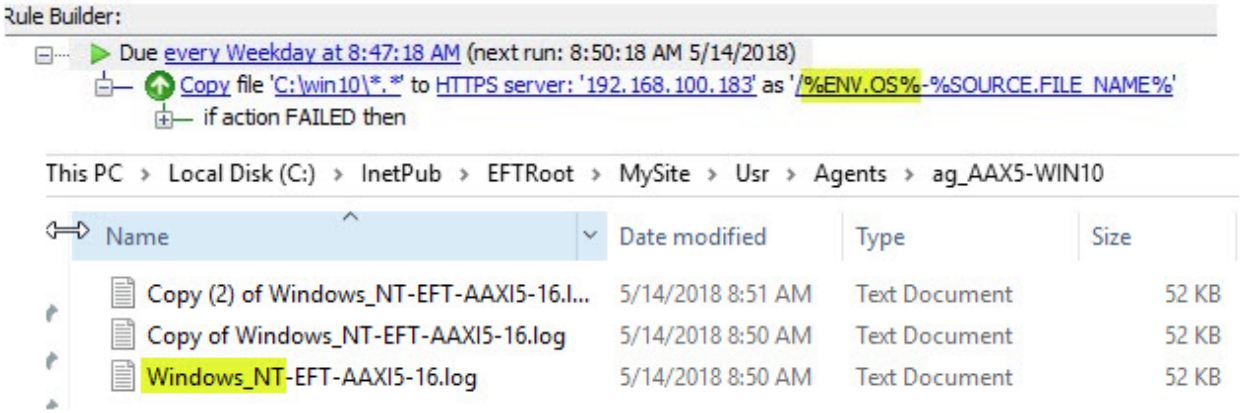
| Text Displayed | Variable | Description |
|---|---|---|
| Remote Agent Name | %AGENT.NAME% | Computer name of remote system running the Remote Agent, enumerated if there is more than one Agent with that name. |
| Remote Agent Version | %AGENT.VERSION% | Version of Remote Agent update |
| Remote Agent Last Update Time Stamp | %AGENT.LAST_UPDATE_TIMESTAMP% | Date of last Remote Agent update |
| Remote Agent Next Update Time Stamp | %AGENT.NEXT_UPDATE_TIMESTAMP% | Date of next scheduled Remote Agent update |
| Remote Agent NetBIOS Name | %AGENT.COMPUTER_NAME% | Computer name of remote system running the agent |
| Remote Agent Template | %AGENT.TEMPLATE% | Template name associated with the Agent |
| Remote Agent Status | %AGENT.STATUS% | Status of Remote Agent (e.g., Active, Pending, Approved, Denied, Banned) |

### RAM Environment Variables

The RAM can make use of environment variables in RAM Event Rules.

- When %ENV.[value]% is used in event rules, EFT will look up the “value” portion from the systems environment variables
- If “ENV.” does not precede the value, then it is not an event rule context variable

- ENV.<variable> can be almost anything. In addition to system variables such as "ENV.OS" you can make up your own variables. In the example below, a file is copied to another server with the type of operating system (OS) prepended to the front of the file name.

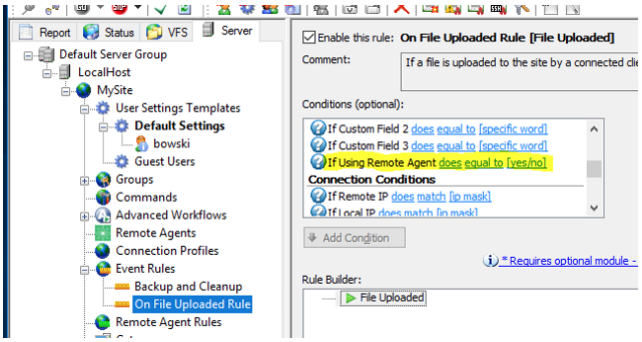



### Remote Agent Event Rule Condition

You can add a "If using Remote Agent does/does not equal to yes/no" to EFT Event Rules for the following events:

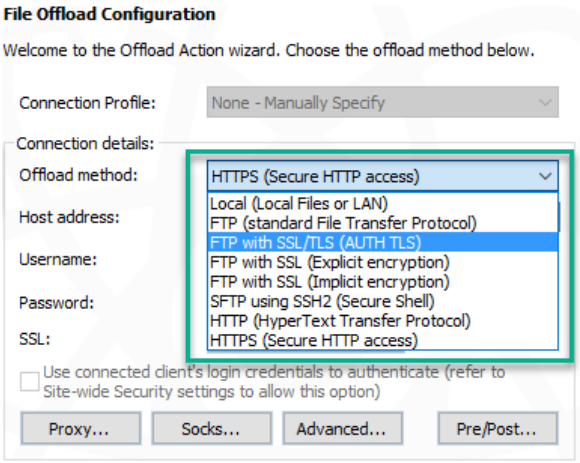
- File Uploaded
- File Downloaded
- File Upload Failed
- File Download Failed
- Before Download

This Condition works for HTTP and HTTPS interactions only.



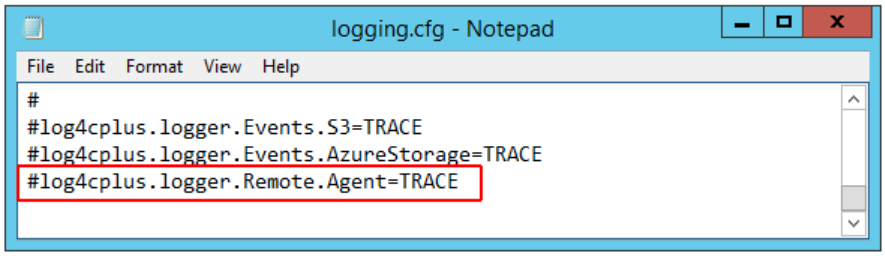

## Sending Files to a Different Server

RAM Agents can send files (download/offload) to another server using RAM Event Rules. By default, all RAM Agents have an HTTPS connection to the EFT that manages that Agent. The EFT administrator can specify a different protocol, host, port, username, and password to allow the Agent to offload (send) files to another EFT or any other server to which you have credentials. Using a Download Action, in the Download Action Wizard, you can specify other protocols, including LAN copy using UNC paths on the local network.




## Remote Agent Logging

On the EFT server, remote Agent events can be tracked in the EFT.log file on EFT. By default, the Remote Agent log is commented out in logging.cfg.




*On the Remote Agent's computer, there is also a file named agent.log that contains updates, errors, event rules it has received, and so on.*

### To enable logging of Remote Agent events

1. On the EFT server computer, open **C:\ProgramData\Globalscape\EFT Server Enterprise\logging. cfg** in a text editor.
2. Scroll to the very bottom, to

   ```
   #log4cplus.logger.Remote.Agent=TRACE and remove the POUND SIGN #
   ```

   TRACE level should be sufficient.

The EFT.log file entries will look something like this:

```
09-07-17 17:07:24,071 [2520] INFO Remote.Agent <> - Template Template (1) added by
admin
09-07-17 17:14:59,634 [2520] INFO Remote.Agent <> - Template Template (2) added by
admin
09-12-17 16:02:39,094 [2524] INFO Remote.Agent <HTTP.ProcessRequest> - Processing
agent initial enrollment request.
09-12-17 16:02:39,203 [2524] INFO Remote.Agent <HTTP.ProcessRequest> - Agent
ag_NUCQT7MG9OH auto-enrolled.
```

Remote Agent activity also appears in the server log file, e.g., **C:\ProgramData\Globalscape\EFT Server Enterprise\Logs\u_ex170912.log**:

```
2017-09-12 21:02:39 192.168.64.141 - - [1]POST /boe/v1/enrollments - 200 345 813 -
443
2017-09-12 21:02:39 192.168.64.141 - - [2]POST /boe/v1/enrollments/6d01ab2a-f523-
4eb1-8b53-d8c608b128b0 - 200 6178 292 - 443
2017-09-12 21:02:39 192.168.64.141 - - [3]POST /boe/v1/agents/6d01ab2a-f523-4eb1-
8b53-d8c608b128b0 - 401 313 216 - 443
2017-09-12 21:02:39 192.168.64.141 - ag_NUCQT7MG9OH [4]user ag_NUCQT7MG9OH - 331 -
- - 443
2017-09-12 21:02:39 192.168.64.141 - ag_NUCQT7MG9OH [4]pass ****** - 200 - - - 443
2017-09-12 21:02:39 192.168.64.141 - ag_NUCQT7MG9OH [4]POST
/boe/v1/agents/6d01ab2a-f523-4eb1-8b53-d8c608b128b0 - 200 3230 299 - 443
2017-09-12 21:02:39 192.168.64.141 - - [5]POST /boe/v1/agents/6d01ab2a-f523-4eb1-
8b53-d8c608b128b0 - 401 313 216 - 443
2017-09-12 21:02:40 192.168.64.141 - ag_NUCQT7MG9OH [6]user ag_NUCQT7MG9OH - 331 -
- - 443
2017-09-12 21:02:40 192.168.64.141 - ag_NUCQT7MG9OH [6]pass ****** - 200 - - - 443
2017-09-12 21:02:40 192.168.64.141 - ag_NUCQT7MG9OH [6]POST
/boe/v1/agents/6d01ab2a-f523-4eb1-8b53-d8c608b128b0 - 200 3230 308 - 443
```

The Remote Agent computer also has logs in **C:\ProgramData\Globalscape\EFT Remote Agent**. Trace-level logging must be enabled in agentlogging.cfg. An administrator can remote access the RAM computer and use a utility such as Baretail to actively monitor what the agent is doing.

C:\ProgramData\Globalscape\EFT Remote Agent\Agent.log

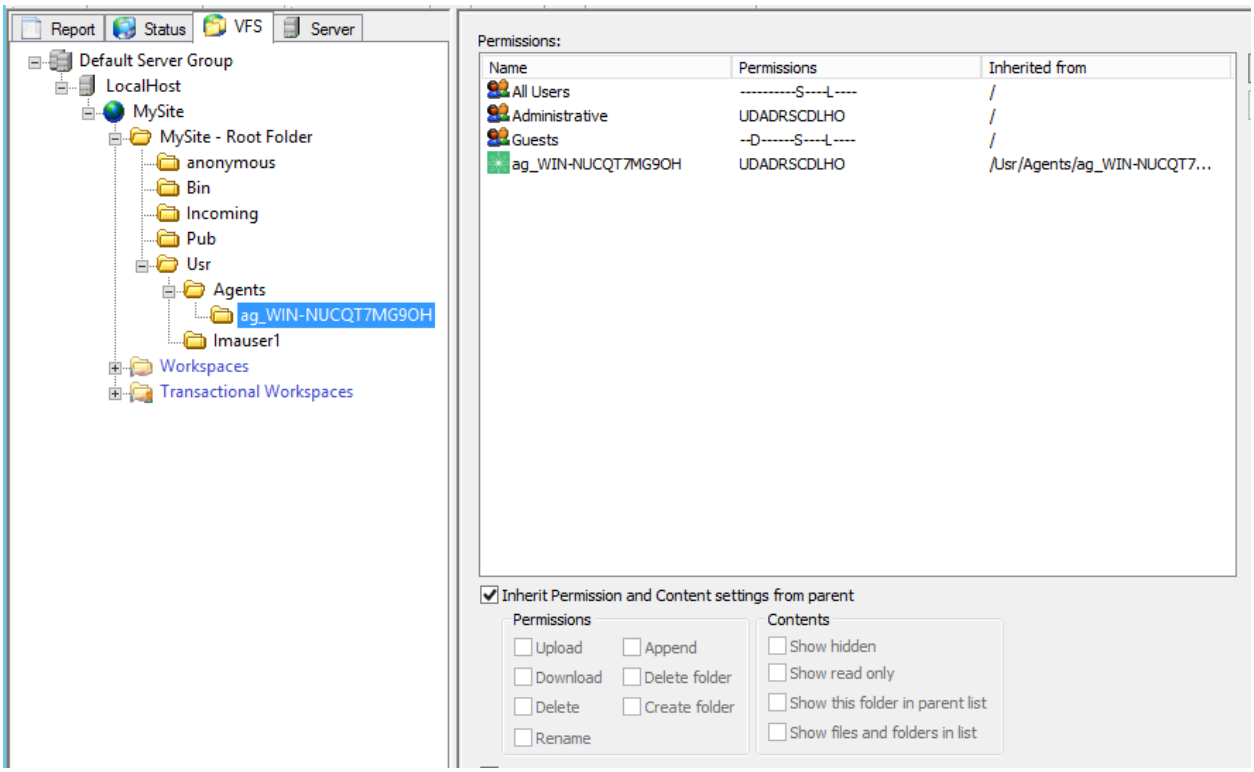
C:\ProgramData\Globalscape\EFT Remote Agent\agentlogging.cfg

More logging on specific transfers in the following directory (similar to how EFT does it by default): C:\ProgramData\Globalscape\EFT Remote Agent\logs\

## Remote Agents in the VFS

After a Remote Agent connects, a home folder for that Agent is created in the VFS. The Remote Agents will each have their own /Usr/ folder in the VFS system. This is important to understand when creating Remote Agent Event Rules.

Each Remote Agent has its own home folder and has every permission so that it can upload, download, create folder, delete files and folders (in its own home folder), rename, and append files. EFT administrators can add/remove permissions via VFS; however, they cannot remove an agent in the VFS.




## Decommissioning Remote a Agent

If you need to remove a Remote Agent so that it no longer connects to EFT, you can decommission it. For example, when upgrading EFT, you must decommission any Remote Agents before upgrading them.

### To decommission a Remote Agent

- In the **Remote agents** pane, click the Remote agent that you want to decommission, then click **Remove**. When the Remote agent checks in for updates, it will decommission itself.