Exchange Service ReadMe and Configuration Setup

Kony Management

October, 2017

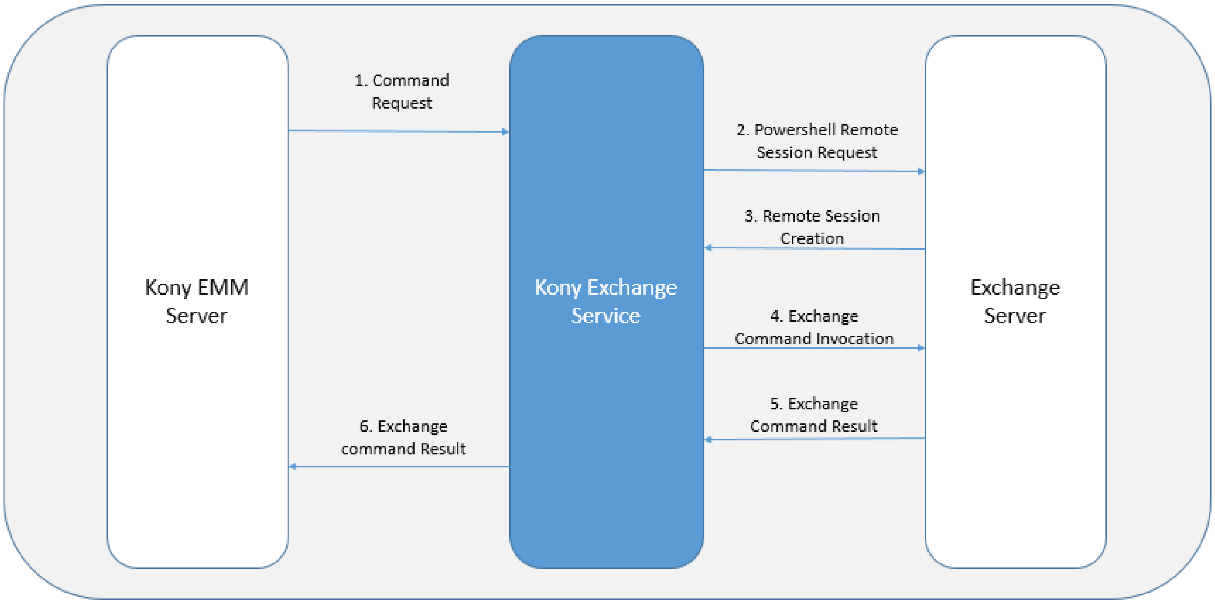
Revision History

Date	Document Version	Description of Modifications/Release
10/09/2017	1.0	Published for V8 Release.

Table of Contents

1. Exchange Service Architecture

Kony Exchange Service helps EMM server to issue Active Sync block or allow emails to devices based on individual device identifiers or device user agents. Below is the high level architecture of the Kony Exchange Service.


Kony EMM Server
1. Command Request
Kony Exchange Service
2. Powershell Remote Session Request
3. Remote Session Creation
4. Exchange Command Invocation
5. Exchange Command Result
6. Exchange command Result
Exchange Server

Kony Exchange Service must be installed on a Windows machine that supports Powershell remoting.

On machines using earlier versions of Windows, install WinRM 2.0 for Powershell remoting if the windows os supports the WinRM installation. All windows operating systems beginning with Windows Vista support Powershell remoting.

Important: Kony does not host Kony Exchange service in Kony cloud deployments of Kony Management suite. You must install the Kony Exchange service in your on premise infrastructure if you want to use Kony Exchange service. Ensure that there is a bidirectional HTTPS connectivity between the Kony Management server hosted on Kony cloud and the Kony Exchange service.

2. ReadMe

`KonyExchPSRemoting.exe` and `KonyExchPSRemoting_HTTP.exe` are windows service executables that can be used to remotely execute exchange server related commands.

> ***Note:*** You can download all files mentioned below in a .zip format from the developer portal.

1. Kony Exchange Service contains the following files:
   a. `KonyExchPSRemoting_HTTP.exe` works only on HTTP.

   b. `KonyExchPSRemoting.exe` works only on HTTPS.

   > ***Note:*** Using HTTPS is recommend instead of HTTP for security.

   c. `instllation.ps1` : User friendly powershell interface takes user inputs, creates the `Config.xml file` and then starts the service.

   d. `restartService.ps1` : Stops and starts the service if it was started by `installation.ps1`script.

   e. `stopService.ps1` : Stops the service if it was started by `installation.ps1` script.

   f. `uninstallation.ps1`: Uninstalls the service if it was started by `installation.ps1`script.

   g. `InstallAndStartHTTP_Service.ps1` : Script installs HTTP Service automatically with the name `konyExchService_http`. This should be used when the `Config.xml` is already prepared to hold the desired values.

   h. `InstallAndStartHTTPS_Service.ps1` : Script installs HTTPS Service automatically with the name `konyExchService_https`. This should be used when the `Config.xml` is already prepared to hold the desired values.

i. `Uninstall_HTTP_Service.ps1` : Uninstalls the service if it was started by `InstallAndStartHTTP_Service.ps1`script.

j. `Uninstall_HTTPS_Service.ps1`: Uninstalls the service if it was started by `InstallAndStartHTTPS_Service.ps1` script.

k. `ConfigurationSetup.txt` : Contains steps for configurations to be done before installing the service.

> ***Note:*** EMM Server only supports multi-tenant configuration even if the environment has only one Exchange Server.

2. Read the `ConfigurationSetup.txt` file and follow the instructions. **Exchange Server** instructions are followed at the Enterprise Exchange Server. **Exchange Remoting Service Machine** related instructions should be followed on the machine on which this service is installed.These are one time changes that need not be repeated for every enterprise service installation.

3. Run the `instllation.ps1`using powershell. The script takes following inputs from the user.

   a. **Enter the Service Name**: Enter the name with which the service should be launched. This leads to the creation of a file named `ServiceName.txt` that contains the name of the service. It is recommended to use the tenant(Enterprise) name as the service name for easy identification.

   b. **Do you want the service to log messages?** Based on your choice, enter y or n. **y** is helpful to debug any issue.

   c. **Enter this Service's key**: This key is stored by Kony console to authenticate with this service.

   d. **Enter this Service's shared secret**: This shared secret is stored by Kony console to authenticate with this service.

e. **Enter session failure retry count (It is a number between 1 and 20, the default value is 3)**: Enter a number. Entering invalid values set it to the default. This value indicates the number of attempts the service tries to connect to the Enterprise exchange server before giving up in case of failure.

f. **Enter the maximum time in seconds the service should wait for the session to form (This value is in seconds between 150 and 1000, and the default value is 150)**: While forming, Sessions take time and this value represents the number of seconds the service should wait for the session to form. If sessions are not established within this specified time limit, the service consider it as a failure and cancels the session establishment and fails the command.

g. **Enter the port on which this service should listen**: Enter a convenient port number. Ensure that this port is not already used on the machine.

h. **Enter the time period (in hours) for GUID Generation (a number between 0 and 24, default value is 3)**: This value represents the time period in hours for token generation.

i. **Enter the maximum number of Powershell sessions to maintain at a time (The default value is 10. Enter a value between 0 and 30)**: This value represents the number of sessions the service will keep alive at a time. Based on the RAM size of the instance on which the service is launched, this setting should be decided. More sessions at given point of time implies that more RAM is used.

   This value should not exceed the value specified by the WSMan configuration MaxShellsPerUser.

   For more information refer to this link: http://msdn.microsoft.com/en-us/library/ee309367(v=vs.85).aspx

   MaxShellsPerUser value should not be altered after this Service is started. Altering this value while service is running may cause unexpected behavior by the service. To alter this value, this service should be stopped, the value should be altered and the service should be restarted.

j. **Enter the queue size (default value is 100)**: This represents the queue size of commands in pipeline if you select the multitenant option.

k. Entering all the above values lead to the creation of a `Config.xml` file in the same directory with the following format:

```
<Config>

<Logging>true</Logging>

<SessionRetryCount>3</SessionRetryCount>

<ExchServicePort>8443</ExchServicePort>

<GUIDGenerationTimePeriod>1</GUIDGenerationTimePeriod>

<MaxPowerShellSessions>3</MaxPowerShellSessions>

<MyKey>key</MyKey>

<MySharedSecret>secret</MySharedSecret>

</Config>
```

l. After the service starts, modify the `Config.xml` to encrypt the key and secret. For example,

```
<Config>

<Logging>true</Logging>

<SessionRetryCount>3</SessionRetryCount>

<ExchServicePort>8443</ExchServicePort>

<GUIDGenerationTimePeriod>1</GUIDGenerationTimePeriod>

<MaxPowerShellSessions>3</MaxPowerShellSessions>
```

```
<MyKeyEnc>encryptedkey</MyKeyEnc>
<MySharedSecretEnc>encryptedsecret</MySharedSecretEnc>
</Config>
```

Note: All values can be altered in the Config.xml except key and secret and the service should be restarted to reflect the new changes. To feed in new key the Config.xml should be opened and the key should be added within the xml tag "MyKey" like this <MyKey>myNewKey</MyKey>. Likewise to add a new secret, it should be added within the xml tag "MySharedSecret" like this <MySharedSecret>myNewSharedSecret/MySharedSecret>. For changing SessionRetryCount, you must add 1 to the desired value. For example, if you want the session retrials to be 3, enter 4 to the SessionRetryCount tag. The Config.xml will look like this before starting the service:

```
<Config>
<Logging>true</Logging>
<SessionRetryCount>3</SessionRetryCount>
<ExchServicePort>8443</ExchServicePort>
<GUIDGenerationTimePeriod>1</GUIDGenerationTimePeriod>
<MaxPowerShellSessions>3</MaxPowerShellSessions>
<MyKeyEnc>encryptedkey</MyKeyEnc>
<MySharedSecretEnc>encryptedsecret</MySharedSecretEnc>
<MyKey>myNewKey</MyKey>
<MySharedSecret>myNewSharedSecret/MySharedSecret>
```

```
</Config>

Once the service is started, the service will pick the new
key and secret values and encrypt them and store back to the
Config.xml file.

<Config>
<Logging>true</Logging>
<SessionRetryCount>3</SessionRetryCount>
<ExchServicePort>8443</ExchServicePort>
<GUIDGenerationTimePeriod>1</GUIDGenerationTimePeriod>
<MaxPowerShellSessions>3</MaxPowerShellSessions>
<MyKeyEnc>newencryptedkey</MyKeyEnc>
<MySharedSecretEnc>newencryptedsecret</MySharedSecretEnc>
</Config>
```

4. Once a port number has been chosen for the option "Enter the port on which this service should listen on" asked by the powershell script, ensure that the port is enabled for HTTPS (in case KonyExchPSRemoting.exe executable was chosen). To bind a port with a SSL certificate for secure communication (https):
    a. For windows 2003, download **Windows 2003 SP1 Support Tools** at http://www.microsoft.com/en-us/download/details.aspx?id=7911

These tools contain a tool `httpcfg.exe` ,which allows to bind port with a SSL Certificate.

For more information about the tool refer: http://msdn.microsoft.com/en-us/library/ms733791.aspx

For newer OS, `httpcfg.exe` is obsolete and replaced with `netsh.exe` as given at:-http://msdn.microsoft.com/en-us/library/windows/desktop/aa364478(v=vs.85).aspx

b. For new OS (2008, Vista) powershell command can be used to bind a port with SSL Certificate. For more information refer: http://msdn.microsoft.com/en-us/library/ms733791.aspx

> ***Note:*** Exchange Service application id is `ee8f0c79-9fbf-4adc-87ae-bfe512a4af02`

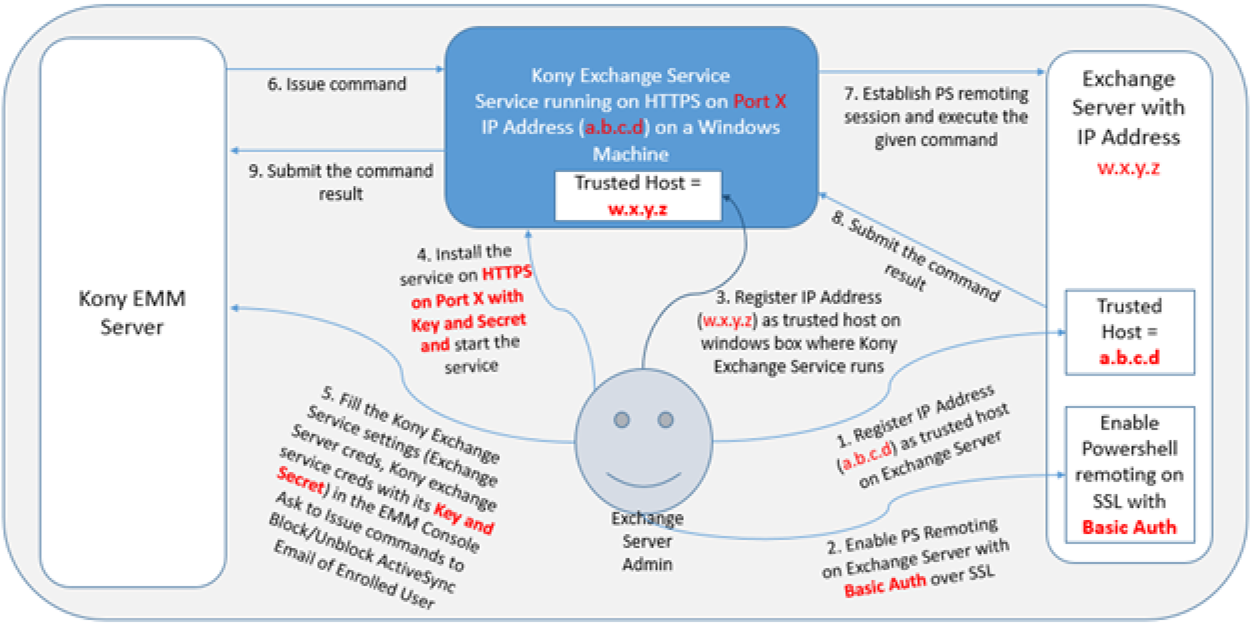
5. Once you finish all the steps, ensure that the service starts successfully and exchange server session is successful. These can be checked from the windows event viewer. If you enter Y for the Logging option (Do you want the service to log messages?), the log with the given service name is present.

2.1 Kony Exchange service flow

The following images display the security recommendations and command flow for the Kony Exchange Service.

2.1.1 Exchange Service Security Recommendations

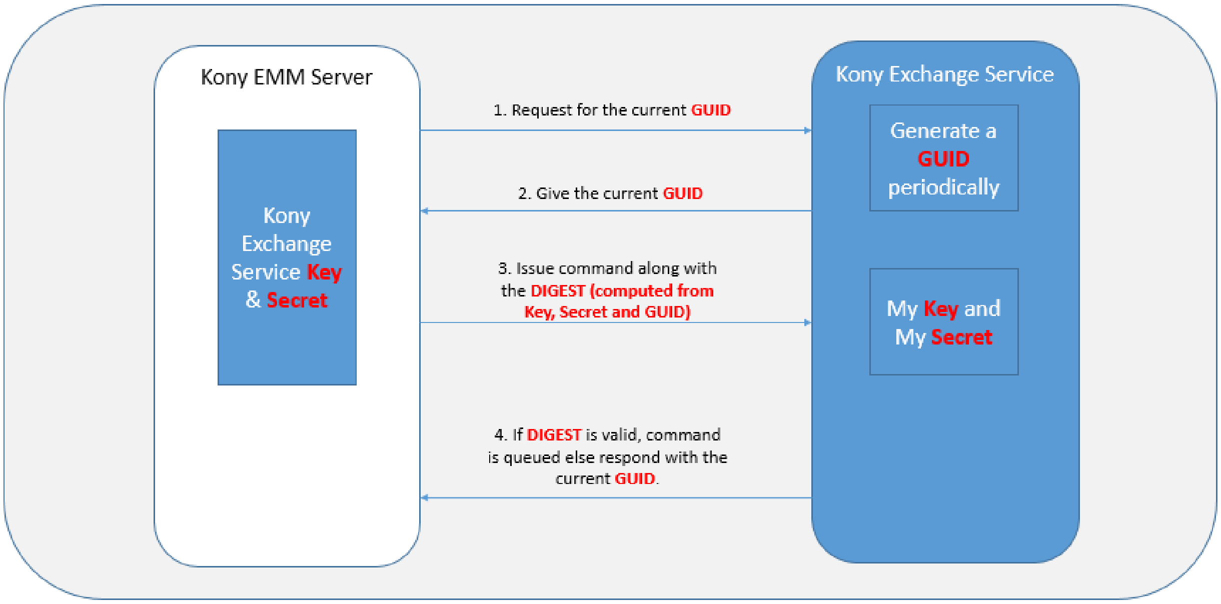
The following image displays flow of commands between EMM server and the Enterprise Exchange server.


Kony EMM Server
6. Issue command
9. Submit the command result
Kony Exchange Service
Service running on HTTPS on Port X
IP Address (a.b.c.d) on a Windows Machine
Trusted Host = w.x.y.z
7. Establish PS remoting session and execute the given command
Exchange Server with IP Address w.x.y.z
8. Submit the command result
Trusted Host = a.b.c.d
Enable Powershell remoting on SSL with Basic Auth
4. Install the service on HTTPS on Port X with Key and Secret and start the service
3. Register IP Address (w.x.y.z) as trusted host on windows box where Kony Exchange Service runs
5. Fill the Kony Exchange Service settings (Exchange Server creds, Kony exchange service creds with its Key and Secret) in the EMM Console
Ask to Issue commands to Block/Unblock ActiveSync Email of Enrolled User
Exchange Server Admin
1. Register IP Address (a.b.c.d) as trusted host on Exchange Server
2. Enable PS Remoting on Exchange Server with Basic Auth over SSL

Note: Points 1 to 5 describe pre-configuration and you should perform them only once. Points 6 to 9 are executed as and when the administrator issues block or unblock command through the EMM console.

2.1.2 Security between Kony EMM Server and Kony Exchange Service

The following image displays the security between the Kony EMM server and Kony Exchange Service.


Kony EMM Server
Kony Exchange Service Key & Secret
Kony Exchange Service
Generate a GUID periodically
My Key and My Secret
1. Request for the current GUID
2. Give the current GUID
3. Issue command along with the DIGEST (computed from Key, Secret and GUID)
4. If DIGEST is valid, command is queued else respond with the current GUID.

From 3.5 GA release, while transporting credentials to the Kony Exchange Service, the Exchange Server credentials are encrypted. These credentials are not decipherable even when http is used by the Kony Exchange Service. Kony recommends to use https communication for security.

3. Configuration Setup

This section describes the configuration steps to be performed on the exchange server as well as on the Windows instance on which the service is installed. Usually Exchange server settings are taken care by the Enterprise hosting the exchange server.

3.1 On Exchange Server Machine

1. Enable powershell remoting using the "Enable-PSRemoting" cmdlet. Ensure that you have admin privileges before you execute this command. For more information, refer http://technet.microsoft.com/en-us/library/hh849694.aspx

2. Set trusted hosts. This includes a list of ip addresses or DNS names from which you need to entertain powershell remoting.

   Powershell console commands are:

   `cd WSMan:\localhost\Client`: This will move to the WSMan Client policy directory.

   `Set-Item .\TrustedHosts *: "*"` will allow all. If specific IPs or DNS addresses are present; add the values separated by commas.

3. Allowing/Disallowing unencrypted traffic:
   Unencrypted traffic means using HTTP. If remoting has to work over HTTP, use the following commands:

   ```
   cd WSMan:\localhost\Client: This will move to the WSMan Client
   policy directory.
   Set-Item .\AllowUnencryptedTraffic $true:  This will allow the
   session to work without encryption.
   ```

   After executing the above mentioned commands on powershell, open **IIS Server Manager> Sites>Default Web Site>Powershell** and disable SSL. Enable Basic authentication.

   Disallowing unencrypted means using HTTPS. The commands are as follows:

```
cd WSMan:\localhost\Client
Set-Item .\AllowUnencryptedTraffic $false
```

After executing the above mentioned commands on powershell, open **IIS Server Manager> Sites>Default Web Site>Powershell** and enable SSL. Enable Basic authentication.

4. Restart the IIS Server.

5. Restart the WinRM Service. Powershell cmdlet for this is Restart-Service WinRM

> ***Note:*** If requests to the Exchange Server are passing through a load balancer, execute exchange server configuration steps on all nodes under the load balancer.

3.2 On Exchange Remoting Service Machine(runs Exchange Service for remoting)

If the Kony remoting service is launched on a different machine, follow the steps given below else directly move to Step no. 6.

> ***Important:*** From Kony Management 3.5.1 onwards, SSLv3 protocol is not supported for HTTPS connections. TLS 1.2 protocol is used. You must install Kony Exchange Service on a computer that has Windows operating system that supports TLS 1.2 protocol (Supported on Windows 7 or higher versions).

1. Enable powershell remoting using the "Enable-PSRemoting" cmdlet. Ensure that you have admin privileges before you execute this command.

   For more information, refer http://technet.microsoft.com/en-us/library/hh849694.aspx

2. **Set trusted hosts**: This includes a list of ip addresses or DNS names to which you do powershell remoting.

```
Powershell console commands are:
cd WSMan:\localhost\Client : This will move to the WSMan Client
policy directory.
Set-Item .\TrustedHosts * : "*" will allow all. Incase Exchnage
Servers IP/DNS is supposed to be trusted add it inplace of "*"
```

> ***Note:*** If there are multiple trusted hosts, separate them by commas.

3. Allowing/Disallowing unencrypted traffic
   Unencrypted traffic means using HTTP. In case remoting has to work over HTTP, use the following commands:

   ```
   cd WSMan:\localhost\Client: This will move to the WSMan Client
   policy directory.
   Set-Item .\AllowUnencryptedTraffic $true: This will allow the
   session to work without encryption
   ```

   After executing the above mentioned commands on powershell, open **IIS Server Manager> Sites>Default Web Site>Powershell** and enable SSL.

   Disallowing unencrypted means using HTTPS. The commands are as follows:

   ```
   cd WSMan:\localhost\Client
   Set-Item .\AllowUnencryptedTraffic $false
   ```

   After executing the above mentioned commands on powershell, open **IIS Server Manager> Sites>Default Web Site>Powershell** and disable SSL.

4. Install the Kony Exchange Service. During the service installation, feed in appropriate values. If powershell is enabled to work on HTTPS in the server configuration, give the Exchange Server URL like https://<hostname>/powershell/ else it appears like http://<hostname>/powershell/

> ***Note:*** Execute the following command in the Powershell console as an administrator to confirm that Powershell remoting is successful. `New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri <your exchange server Poweshell URI> -Credential <your user logon> -Authentication Basic -AllowRedirection` Enter password when prompted. Session details will appear on the console

> ***Note:*** For Exchange in Office365, the Exchange Server powershell URL is https://outlook.office365.com/powershell. For more information refer to http://technet.microsoft.com/en-us/library/jj984289(v=exchg.150).aspx