Deployment Guide
Mar-2016 rev. a

Integrating the Array Standalone Client with RSA Token Automation

Table of Contents

1 Introduction

Array’s AG Series secure access gateways offer two methods of network access: Through a Web client or through a standalone client. This document introduces how to integrate the Array Standalone Client with the RSA token automation. Only the Array Standalone Client for Windows supports this function.

With this function, when the end user tries to establish a VPN connection via the Array Standalone Client, they only need to enter the PIN code instead of the token code or passcode. The Array Standalone Client will obtain the token code or passcode via the SDK provided by RSA. To ensure the SDK works normally, the RSA SecurID Token Client must be installed and the valid token file must be imported.

The process of integrating the Array Standalone Client with the RSA SecurID software token consists of the following steps:

Install the RSA SecurID Token Client

Import the token file to the RSA Token Client

Install the Array Standalone Client

Run the Array Standalone Client

The following sections will describe these steps in detail.

2 Install the RSA SecurID Token Client

The administrator can download the installation package for the client from the official RSA website and deliver it to end users:

After obtaining the installation package, end users should:

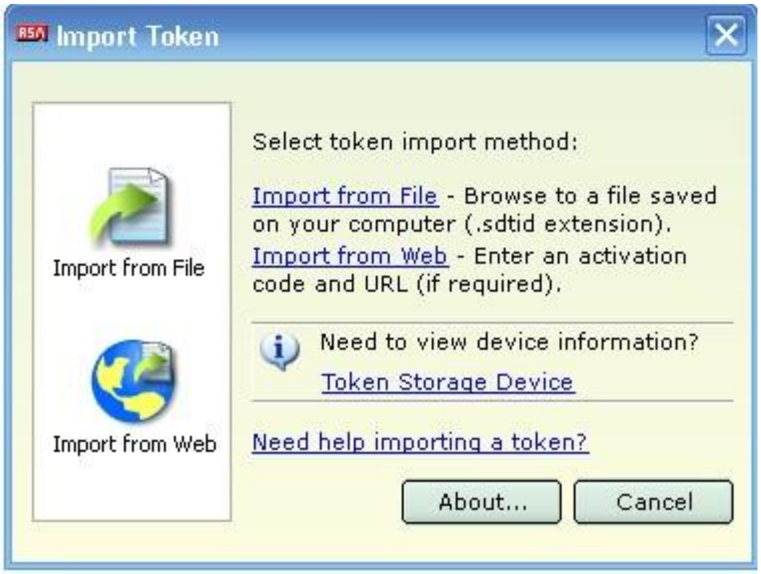
Run “RSASecurIDTokenAuto411.msi” to install the RSA SecurID Token Client on 32-bit Windows OS.

Run “RSASecurIDTokenAuto412x64.msi” to install the RSA SecurID Token Client on 64-bit Windows OS.

3 Import the Token File to RSA SecurID Token Client

To import the token file to the RSA SecurID Token Client, end users should do as follows:

1. Obtain the token file from the administrator such as “tongjj_000147233970.sdtid”.
2. In the Import Token window, click the **Import from File** action link, as shown in the following figure.



Select token import method:

Import from File - Browse to a file saved on your computer (.sdtid extension).

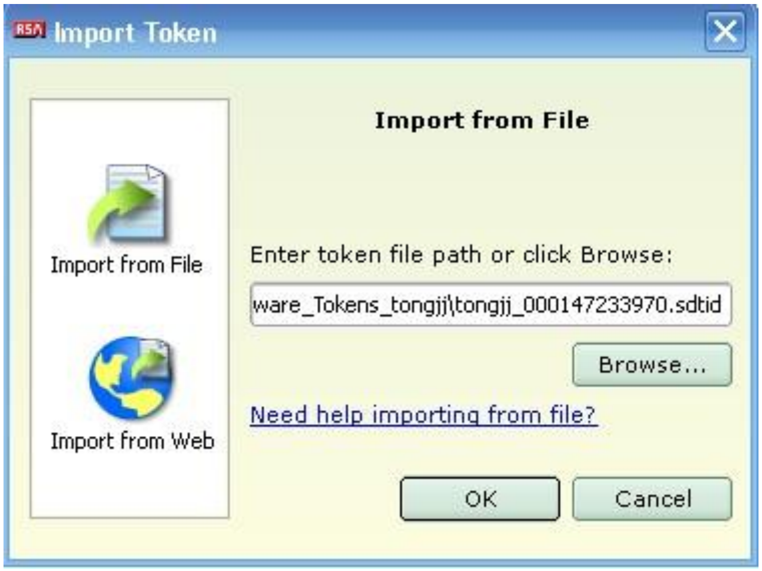
Import from Web - Enter an activation code and URL (if required).

Need to view device information?

Token Storage Device

Need help importing a token?

3. Specify the path of the token file and click the **OK** button, as shown in the following figure.



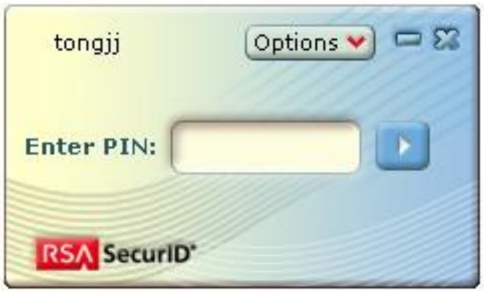
Import from File

Enter token file path or click Browse:

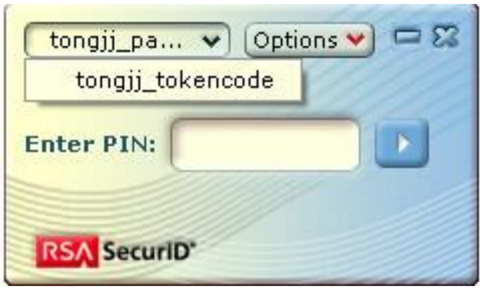
ware_Tokens_tongjj\tongjj_000147233970.sdtid

Need help importing from file?

4. After the token file is imported, the token file name will be the only name displayed on UI of the RSA SecurID Token Client, as shown in the following figure.



5. If more than one token file is imported, all the token files can be seen on the UI, as shown in the following figure.



After the token files are imported, end users can exit the RSA SecurID Token Client. The Array Standalone Client can obtain the token code or passcode even when the RSA SecurID Token Client is not running.

4 Install the Array Standalone Client

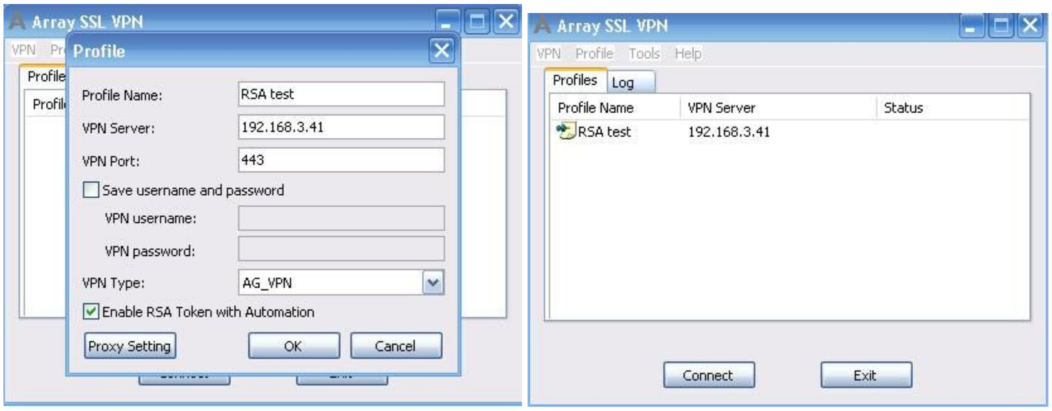
The administrator can download the Array Standalone Clients installation packages from the Array support site and deliver them to end users: https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/downloads/downloads.html

After obtaining the installation packages, end users should:

Run SSLVPNSetup.exe in the SSLVPNSetup_win32.zip package to install the Array Standalone Client on 32-bit Windows OS.

Run SSLVPNSetup_x64.exe in the SSLVPNSetup_win64.zip package to install the Array Standalone Client on 64-bit Windows OS.

When creating the profile for the virtual site on the Array Standalone Client, end users should select the **Enable RSA Token with Automation** check box, specify other parameters and click the **OK** button, as shown in the following figure.



Profile Name: RSA test

VPN Server: 192.168.3.41

VPN Port: 443

□ Save username and password

VPN username:

VPN password:

VPN Type: AG_VPN

☑ Enable RSA Token with Automation

Profile Name	VPN Server	Status
RSA test	192.168.3.41	

After the check box is selected, end users only need to input the PIN code instead of the passcode or token code, and the Array Client will generate the passcode or token code according to the input PIN code.

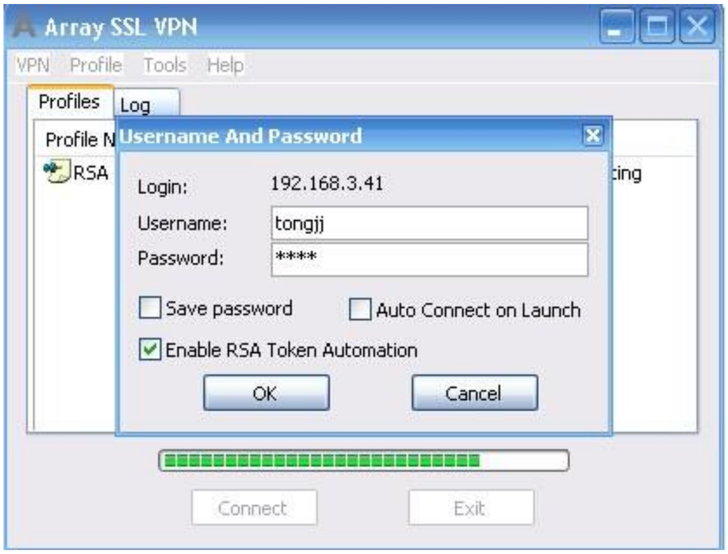
Note:

This check box can be selected only when the virtual site uses RSA authentication only or as one factor of the multi-factor authentication.

The administrator can customize the Array Standalone Client to make this check box selected by default by modifying the OEM.ini file as follows before delivering the installation package to end users:

RSATokenAutomation=1 (value: 1-enable, 0-disable; defaults to 1)

In this case, if the authentication method the virtual site uses is not RSA (such as LocalDB) the end user needs to clear this check box during authentication and enter the correct username and password, as shown in the following figure.



Login: 192.168.3.41

Username: tongjj

Password: ****

□ Save password □ Auto Connect on Launch

☑ Enable RSA Token Automation

5 Run the Array Standalone Client

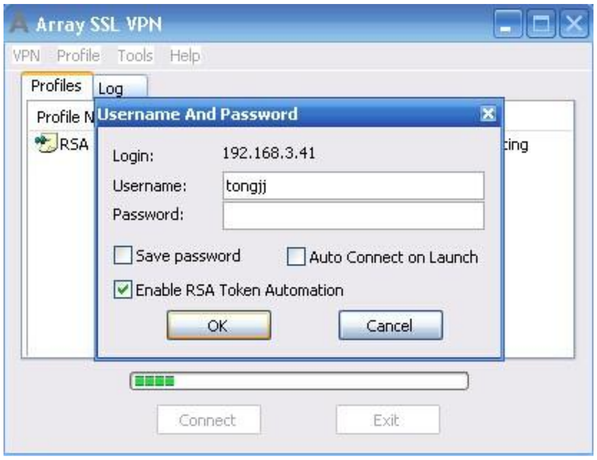
Before running the Array Standalone Client, users MUST make sure that the time of current client PC is totally the same as that of the RSA server; otherwise, authentication will fail.

a) Only RSA Authentication Used

No PIN

1. Under the **Profiles** tab of the main window, select the profile and click the **Connect** button.

2. In the displayed **Username And Password** dialog box, enter the username in the **Username** text box, leave the **Password** text box empty, and click the **OK** button as shown in the following figure.



Username And Password

Login: 192.168.3.41

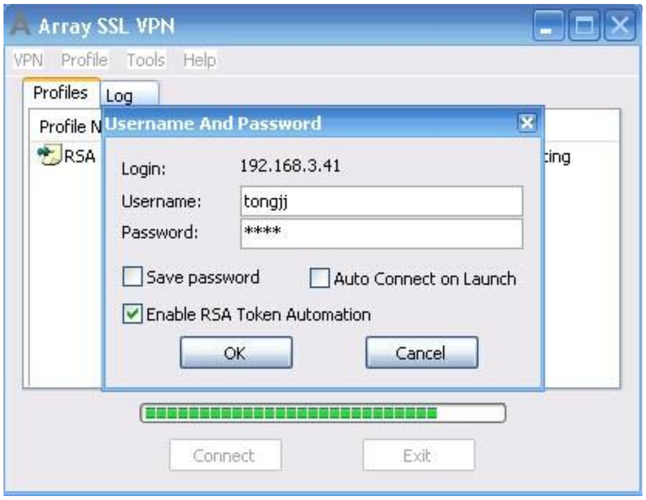
Username: tongjj

Password:

□ Save password □ Auto Connect on Launch

☑ Enable RSA Token Automation

3. In the displayed **Enter your new PIN** dialog box, specify the parameters **New PIN** and **Confirm** and click the **OK** button, as shown in the following figure.



Username And Password

Login: 192.168.3.41

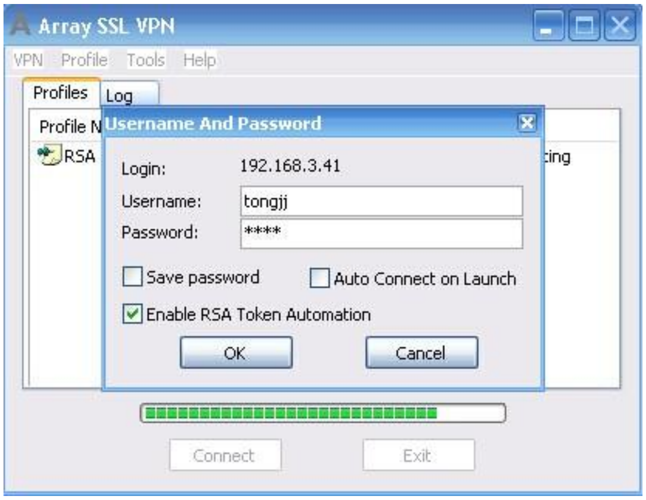
Username: tongjj

Password: ****

□ Save password □ Auto Connect on Launch

☑ Enable RSA Token Automation

Then the Array Standalone Client will perform authentication automatically and establish the VPN tunnel.



Username And Password

Login: 192.168.3.41

Username: tongjj

Password: ****

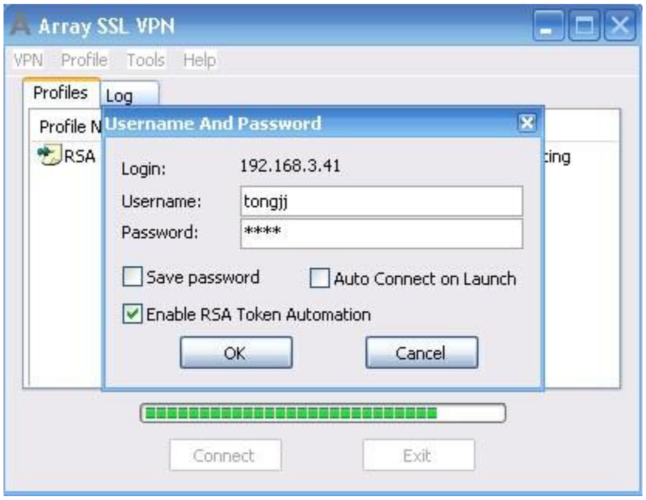
□ Save password □ Auto Connect on Launch

☑ Enable RSA Token Automation

PIN already exists

At subsequent logins, the end user does not need to set the new PIN code.

During the RSA authentication, in the **Username and Password** dialog box, enter the username in the **Username** text box, enter the PIN code in the **Password** text box, and click the **OK** button, as shown in the following figure.



Username And Password

Login: 192.168.3.41

Username: tongjj

Password: ****

□ Save password □ Auto Connect on Launch

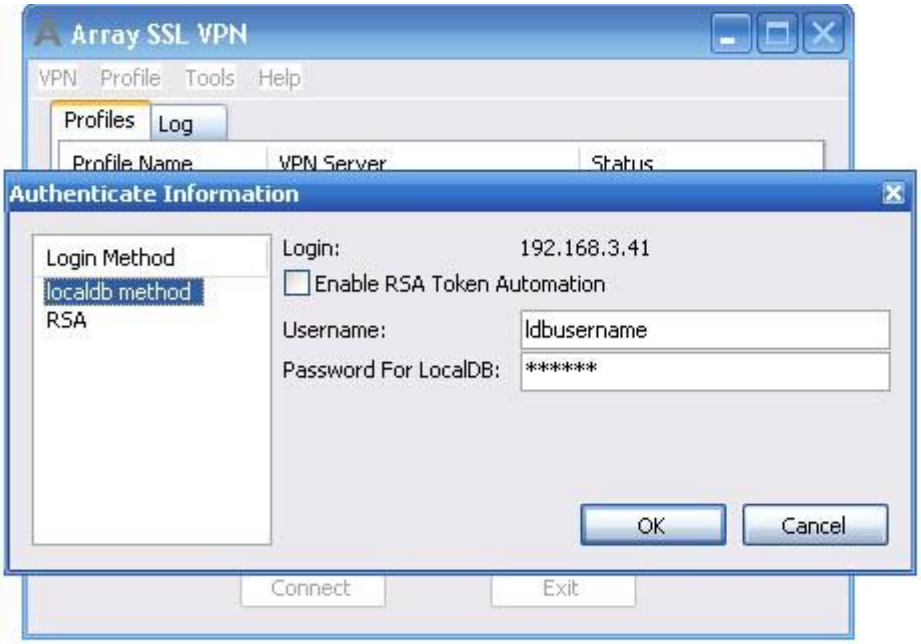
☑ Enable RSA Token Automation

Multi-Factor Authentication Including RSA

This section uses LocalDB+RSA authentication as an example.

No PIN

1. Under the **Profiles** tab of the main window, select the profile and click the **Connect** button.
2. In the displayed **Authenticate Information** dialog box, select the LocalDB method name from the **Login Method** pane, specify the parameters **Username** and **Password for LocalDB** and click the **OK** button, as shown in the following figure.



Login Method
localdb method
RSA

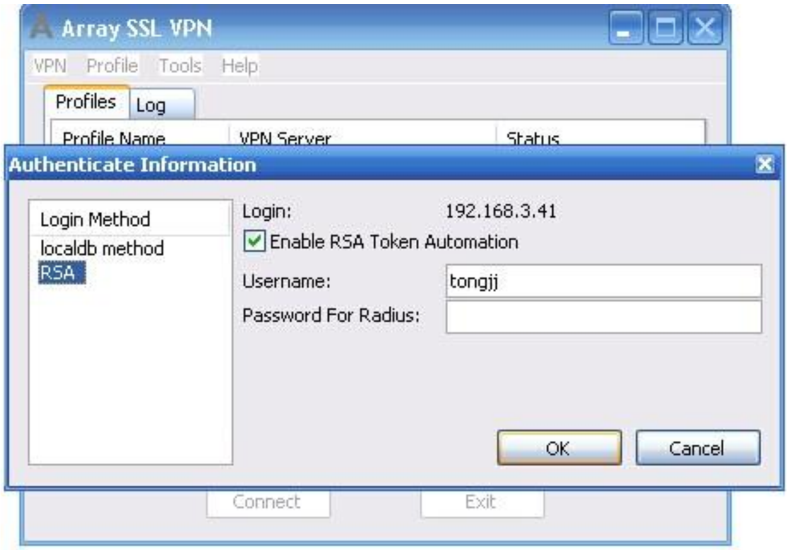
Login: 192.168.3.41

□ Enable RSA Token Automation

Username: ldbusername

Password For LocalDB: ******

3. Select the RSA method name from the **Login Method** pane, specify the parameters **Username**, leave the **Password for Radius** check box empty, and click the **OK** button, as shown in the following figure.



Login Method
localdb method
RSA

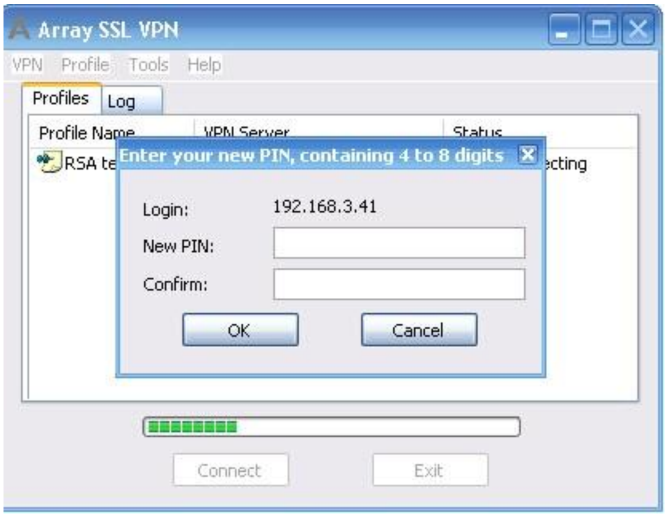
Login: 192.168.3.41

☑ Enable RSA Token Automation

Username: tongjj

Password For Radius:

4. In the displayed **Enter your new PIN** dialog box, specify the parameters **New PIN** and **Confirm**, and click the **OK** button, as shown in the following figure.



Enter your new PIN, containing 4 to 8 digits

Login: 192.168.3.41

New PIN:

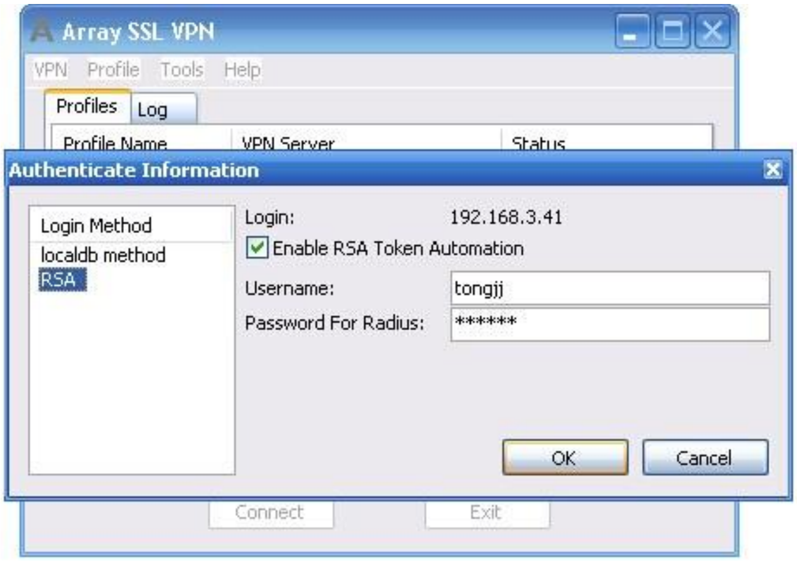
Confirm:

The Array Standalone Client will perform authentication automatically and establish the VPN tunnel.

PIN Already Exists

At subsequent logins, the end user does not need to set the new PIN code.

During the RSA authentication, select the RSA method name from the **Login Method** pane, enter the username in the **Username** text box, enter the PIN code in the **Password for Radius** text box, and click the **OK** button, as shown in the following figure.



Authenticate Information

Login Method
localdb method
RSA

Login: 192.168.3.41

☑ Enable RSA Token Automation

Username: tongjj

Password For Radius: ******

About Array Networks

Array Networks is a global leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore® software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 250 employees worldwide and is a profitable company with strong investors, management and revenue growth. Poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, IDC and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.

Corporate Headquarters
info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

EMEA
rschmit@arraynetworks.com
+32 2 6336382

China
support@arraynetworks.com.cn
+010-84446688

France and North Africa
nsedrati@arraynetworks.com
+33 6 61174433

India
isales@arraynetworks.com
+91-080-41329296

Japan
sales-japan@
arraynetworks.com
+81-44-589-8315

To purchase Array Networks Solutions, please contact your Array Networks representative at 1-866-MY-ARRAY (692-7729) or authorized reseller

Mar-2016 rev. a