Fiberlink Communications Corp
Extend360

RSA SecurID Ready Implementation Guide

Last Modified: 09/16/2009

Partner Information

Product Information	
Partner Name	Fiberlink Communications Corporation
Web Site	www.fiberlink.com
Product Name	Extend360
Version & Platform	2.8.000.99_r32050
Product Description	The Extend360 Agent is a universal wireless client that makes it easy for mobile workers to connect to any type of wireless network, including Wi-Fi hotspots, mobile cellular data networks, and corporate wireless LANs, utilizing RSA SecurID in providing reliable and secure user based two-factor authentication.
Product Category	Networks and Communications

FIBERLINK

Solution Summary

The Extend360 Agent is a universal wireless client that makes it easy for mobile workers to connect to any type of wireless network, including Wi-Fi hotspots, mobile cellular data networks, and corporate wireless LANs.

Fiberlink's patent-pending Active Transport Notification technology detects all available hot spots and wireless access points within range. Mobile employees can choose any authorized connection type from a simple menu bar. A uniform logon eliminates the need for employees to remember multiple passwords and authentication procedures.

Enterprises can consolidate on one wireless agent instead of supporting multiple clients, and can reduce help desk and support costs. Now the Extend360 Agent may also be used in RSA SecurID authenticated 802.1x environments.

The Extend360 Agent has also been integrated with the RSA SecurID Software Token. By integrating the Extend360 with the RSA SecurID Software Token, end users are only required to enter their PIN when authenticating. This solution provides Enterprises the security of 2-factor authentication while giving their users the convenience of logging in with less typing.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
RSA SecurID Library Version Used	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes
RSA Authentication Agent Host Type for 6.1	N/A
RSA Authentication Agent Host Type for 7.1	N/A
RSA SecurID User Specification	N/A
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	Yes (Software Token)

Product Requirements

Product Requirements: Fiberlink Extend360 Agent	
Platform	**Required Patches**
Microsoft XP	All Patch Levels supported
Microsoft Vista	All Patch Levels supported

Additional Hardware Requirements:

The Fiberlink Extend360 Client requires that an RSA Certified 802.1x solution be used as the backend for this integration.

Partner Product Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring the Extend360 Agent

The scope of this guide is to show how to setup and configure the Fiberlink Extend360 Agent to be used in RSA SecurID 802.1x authenticated environments. For a more in depth explanation on how to configure your network switch or wireless hardware, please refer to your administrator or documentation provided by your hardware vendor.

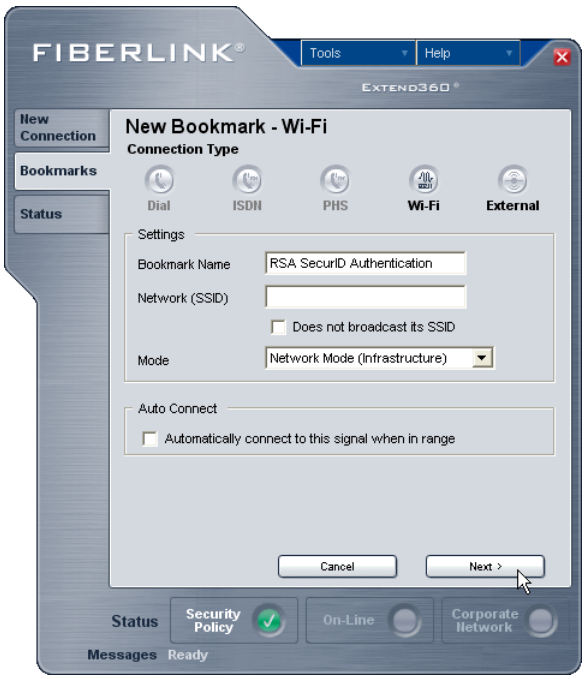
First, install the Fiberlink Extend360 Agent following the Fiberlink product documentation. Once the product is installed launch the Extend360 application.

Create a Bookmark

1. Click the **Bookmarks** tab and select **Wi-Fi**.
2. Click on the button labeled **New**.

3. Enter a **Bookmark Name**.
4. Enter **Network (SSID)** if not auto filled.
5. Select **Network Mode (infrastructure)** from the **Mode** drop down menu.

6. Click **Next**.

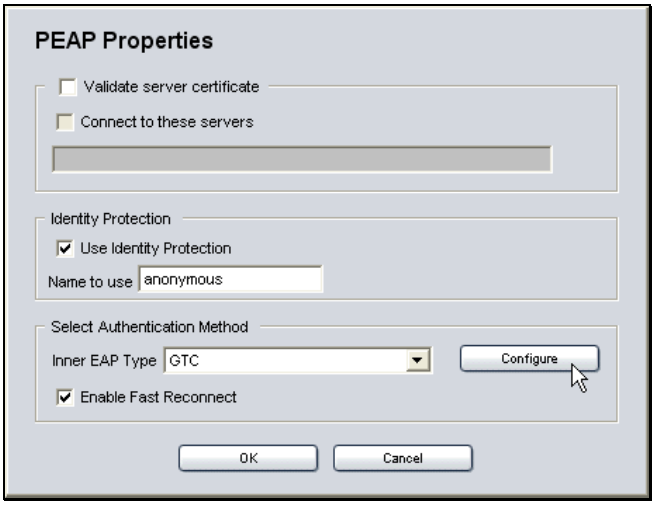


7. Select **802.1x** from the **Network Authentication** menu.
8. Under 802.1x Authentication, select **PEAP** for the EAP Type.
9. Click **Properties** to continue configuring **PEAP**.

10. Click to uncheck **Validate server certificate**.

Note: Check with your Administrator to verify if this box should be checked.

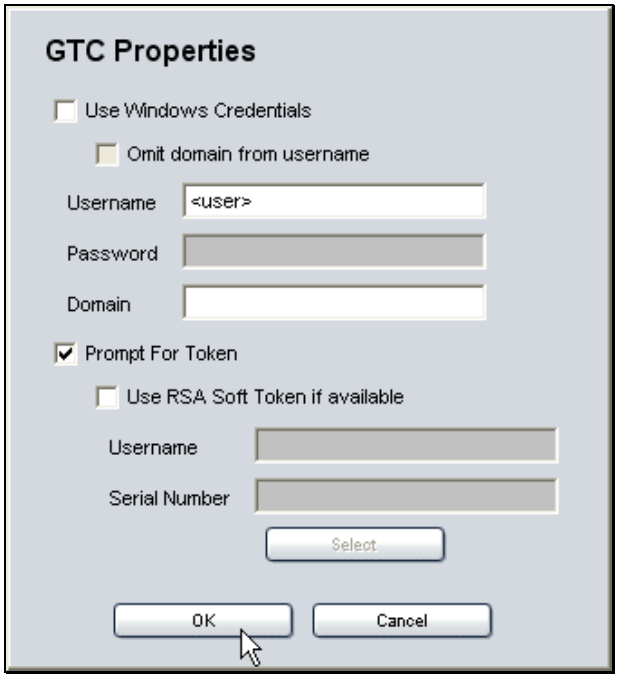
11. Select **GTC** as **Inner EAP Type**.
12. Click the **Configure** button.



13. Click to uncheck the box for **Use Windows Credentials**.

Note: Check with your Administrator to verify if this box should be checked. If checked, you may also need to provide a value for the Domain.

14. Enter the RSA SecurID **Username**.
15. Click to check the box for **Prompt For Token**.



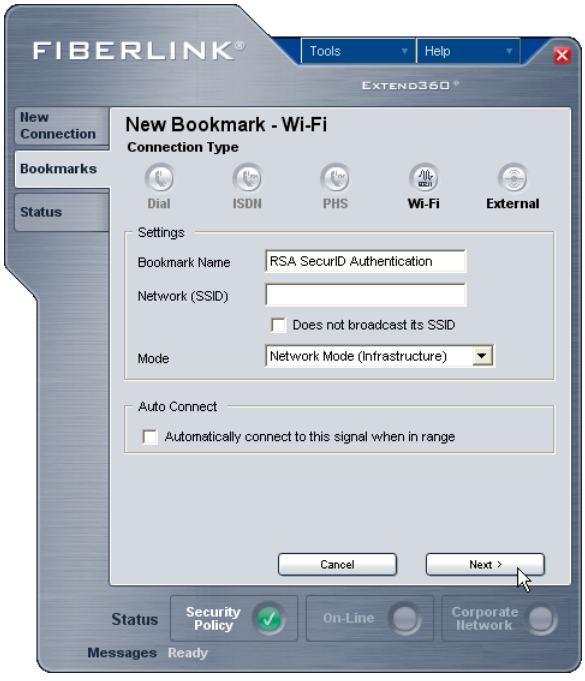
16. Click **OK**, and click **OK** again to return to the **Bookmark** screen.

17. Click **Save** to save your settings as a new bookmark.

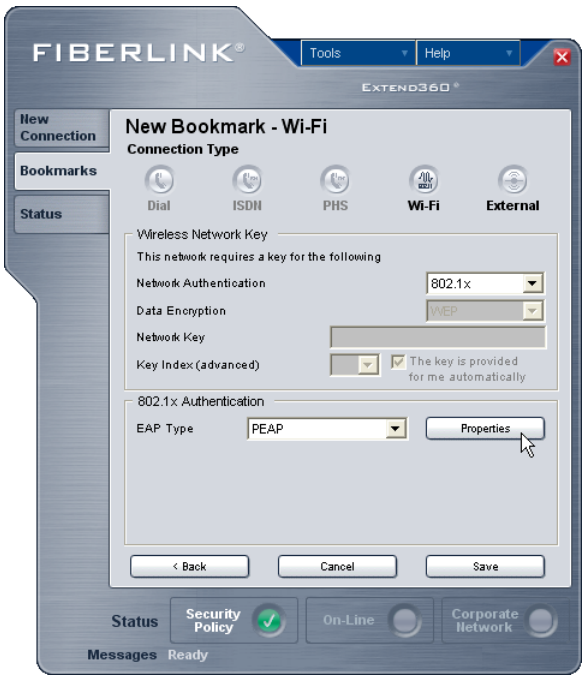
Software Token Automation Configuration

The instructions below rely on having completed the **Create a Bookmark** section.

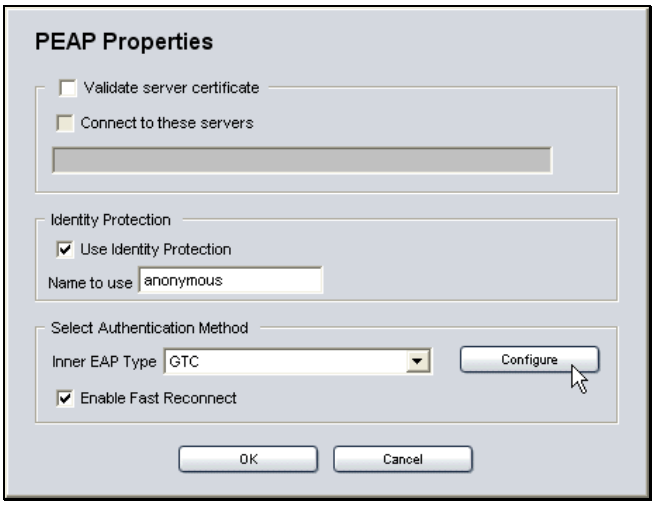
1. Click the **Bookmarks** tab and select the name of the Bookmark created in **step 18** of **Create a Bookmark**.
2. Click on the button labeled **Edit**.
3. Click **Next**.



4. Click **Properties** to configure **PEAP**.



5. Click the **Configure** button for **GTC**.



6. Under the **GTC Properties** dialog, select the checkbox labeled **User RSA Soft Token if available**.

7. Next, click on the **Select** button.

8. From the drop-down list, select the **serial** for the Software Token to be used.

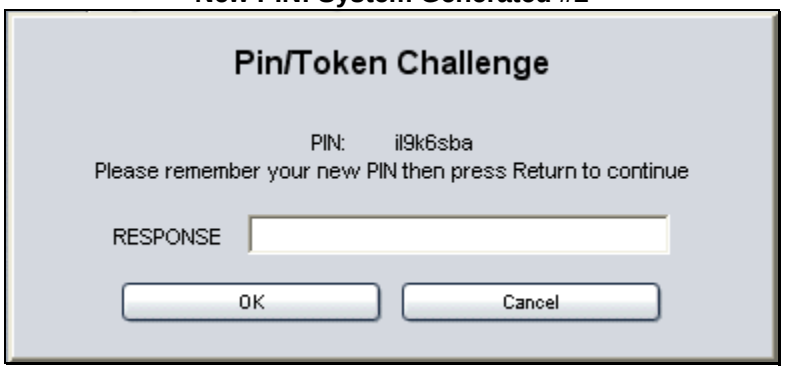
9. Click the **OK** button.

End-user Experience

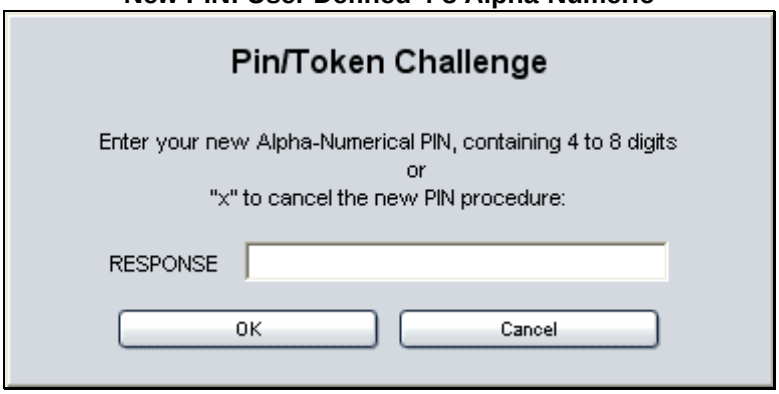
The following are examples of authentication prompts users will see when authenticating

New PIN: System Generated #1

New PIN: System Generated #2



New PIN: User Defined 4-8 Alpha-Numeric



New PIN: User Defined 5-7 Numeric

New PIN: Reenter PIN:

Next TokenCode Mode

Certification Checklist for RSA Authentication Manager 7.x

Date Tested: 09/11/2009

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP2	Windows Server 2003 Enterprise
RSA Software Token	3.0.7	Windows XP Professional
Cisco Aironet Access Point	12.3.7JA2	IOS
Fiberlink Extend360	2.8.000.99_r32050	Windows XP Professional

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny Numeric PIN	N/A	Deny Numeric PIN	✓
PIN Reuse	N/A	PIN Reuse	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Fixed Passcode	N/A	4 Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	✓
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	✓
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

CMY / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

1. **Force Authentication after New PIN:** Force Authentication after New PIN does not occur when using a Cisco ACS RADIUS server. Cisco has been notified of this behavior and plans to address this in a future release.
2. **RSA Software Token and SID800 Tokens in automation mode:** Automation mode for RSA Software Token v4.0 and SID800 is currently not supported. Automation mode will be supported in an upcoming RSA release. Please check with your Administrator regarding availability.

Important: RSA Software Token and SID800 Tokens in manual mode: Manual mode for RSA Software Tokens and SID800 is currently supported and will work as designed. Users will authenticate via the authentication prompts as shown in this document.

Appendix

Please refer to the following RSA Security Implementation Guides for server devices used in this certification testing.

http://www.rsa.com/rsasecured/guides/imp_pdfs/Cisco_WLAN_PEAP_AuthMan7.1.pdf