

# Agent Installation Using Smart Card Credentials Detailed Document

EventTracker 8815 Centre Park Drive Columbia MD 21045 www.eventtracker.com

Publication Date: Sept. 19, 2016

## Abstract

This document is to guide the user to Install/Uninstall or upgrade agent using the Smart Card credentials.

## **Target Audience**

EventTracker user, who are having the Smart Card license.

### Pre-requisite

This utility can be used in the server machine where EventTracker is installed. Thus, the user will have to install the Smart Card driver on Manager Machine and use the Smart Card Device (Smart Card reader and the proper Smart Card) on the same machine.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



## Why to use this update?

In the earlier given Smart Card update, it allowed only authentication for EventTracker application. Thus, while installing or deploying agents, the user was required to authenticate using windows credential. To overcome this limitation, a utility has been provided which will now allow the user to deploy agents using their Smart card credentials.

#### \*\*IMPORTANT

- > The Smart Card user should have proper access rights and permissions on the Remote machine.
- If the Smart card is created for a respective domain and if the user wants to deploy agent in some other domain, he\she should create Domain Trust relationship between the two domains or other multiple domains.

# Steps to be followed after applying the Update: ET82U16-021

- Go to the Install Directory/EventTracker/AdvancedReports folder.
- Double-click the 'Prism.EventTracker.RemoteAgentInstaller.exe" utility.

👪 l 🕞 🛄 = l	Application Tools		AdvancedF	Reports	_		x
File Home Share	View Manage					~	0
📀 🍥 🔻 🕇 <u>)</u> « Pr	ism Microsystems 🔸 EventTracl	ker 🕨 AdvancedR	eports	🗸 🖒 Search	AdvancedReports	۶	>
	hlanna 🔺		Data was differed		Si		
🚖 Favorites	Name		Date modified	Аррисацон еленъ	SIZE		
🛄 Desktop	🚳 Prism.Common.ServiceM	lanager.dll	6/6/2016 1:43 AM	Application extens	39 KB		
🐌 Downloads	🚳 Prism.Converter.dll		6/6/2016 1:43 AM	Application extens	22 KB		
📃 Recent places	🚳 Prism.DescriptionParser.d	11	6/6/2016 1:43 AM	Application extens	27 KB		
	Serism.ErrorLogger.dll		6/6/2016 1:43 AM	Application extens	30 KB		
🜉 This PC	Prism.EventTracker.Collect	ction Point Tool	6/6/2016 1:43 AM	Application	76 KB		
	Nrism.EventTracker.Excel.	Core.dll	6/6/2016 1:43 AM	Application extens	1,109 KB		
📬 Network	🍸 Prism.EventTracker.IPresc	olver	5/17/2016 2:25 AM	Application	46 KB		
	🐉 Prism.EventTracker.Remo	teAgentInstaller	9/8/2016 5:34 AM	Application	130 KB		=
	Prism.EventTracker.Report	rter	6/6/2016 1:43 AM	Application	55 KB		
	🃄 Prism.EventTracker.Repoi	rter.exe.config	2/29/2016 12:18 PM	CONFIG File	1 KB		
	🥝 Prism.EventVaultExplorer:	Search	6/6/2016 1:43 AM	Application	32 KB		
	🚳 Prism.ExportingLibrary.dl	I	6/6/2016 1:43 AM	Application extens	51 KB		
	🚳 Prism.ExpressionParser.dl	I	2/29/2016 12:18 PM	Application extens	30 KB		
	🚳 Prism.Extensions.dll		6/13/2016 1:51 AM	Application extens	20 KB		
	🚳 Prism.FDCCXML.dll		5/23/2016 11:58 AM	Application extens	29 KB		
	🚳 Prism.Generic.API.dll		6/6/2016 1:43 AM	Application extens	541 KB		
	🚳 Prism.IndexerViewer.dll		6/6/2016 1:43 AM	Application extens	44 KB		
	🍸 Prism.IndexerViewerProce	essor	6/6/2016 1:43 AM	Application	38 KB		
	Prism.IndexerViewerProce	essor.exe.config	2/29/2016 12:18 PM	CONFIG File	1 KB		
	🚳 Prism.Infrastructure.dll		6/6/2016 1:43 AM	Application extens	39 KB		
	🚳 Prism.IPClassification.dll		6/6/2016 1:43 AM	Application extens	22 KB		~
92 items   1 item selected	129 KB					:==	





The following screen gets displayed:

CTION	COMPUTER LIKE	COMPUTER LIKE									
Vone 🔹		GO All Agent 🗌 All Change Audit									
Group Name	System name	IP Address Agent	version Agent CA versio	n Change Audit	Port No	Device Type					
ll groups	BAGHEERA	192.100.1004	Г	Г	0	Win 10					
llert	вов	192.100.1.100			0	Win 10					
efault	CACOFONDC	192.100.1.100	Г	Г	0	XP Pro					
omain Controllers	CASPER	192.100.1.113			0	Win 7					
ventTracker	CHIPDALE	192.111.111	Г	Г	0	Win 7					
irewall Devices	CINDERELLA	192.1.1.1.1.1.1			0	Win 10					
PTEAM	DALE	192.100.1.00	Г	Г	0	2012 R2					
letwork Devices	DBSERVER-PC	192.100.1.71			0	Win 7					
NPL	DEXTER	192.100.1.102	Г	Г	0	2008 R2					
IEM1	DUCKTALES	192.100.1.100			0	Win 10					
UPPORT	ELC	192.100.1.77			0	Win 8.1					
est123	ESXVCSERVER	192.100.1115			0	2003					
OONS	ESXWIN2K12R2VM3	192.100.1.100			0	2012 R2					
/mWare	ESXWIN2K3R2VM3	192.100.1.170			0	2003					
/in 7 and Server 2008 Above	ESXWIN2K8R2VM1	192.100.1.200			0	2012 R2					
Vin XP and Server 2003	ESXWIN2K8R2VM3	192.100.100			0	2008 R2					
	ESXWIN2K8R2VM7	192.100.1.117			0	2008 R2					
	ESXVVIN2K8VM1	192.100.1.59			0	2008					
	ETSBI02	192.111.1115			0	2012 R2					
	EXCHTEST	192.100.110			0	2003					
	FELDK	192.100.1.102			0	Win 7					
	GENIE	192.100.100			0	Win 10					
	HERCULES	192.100.000			0	Win 10					

Figure: 2

**NOTE**: Only the windows systems will be listed along with their IP Addresses.

#### To Install an Agent,

- In the Action field, select Install Agent/Start Poll from the dropdown list.
- Select the Group from the **Group Name** pane.

All the systems get listed.



Agent Utility						/			
ACTION	COMPUTER LIKE								Installat
Install agent/Start poll 🔹			GO	🗆 All Agent 🗆 i	All Change Audi	t		Clear	
Group Name	System name	IP Address	Agent version	Install Agent	CA version	Install CA	Port No	Device Type	
All groups	BAGHEERA	192.100.1.104					0	Win 10	
Alert	BOB	192.100.1.120					0	Win 10	
Default	CACOFONIX	192.100.1.103					0	XP Pro	
Domain Controllers	CASPER	192.100.1.110					0	Win 7	
EventTracker	CHIPDALE	192.100.1.01					0	Win 7	
Firewall Devices	CINDERELLA	192.100.1.171					0	Win 10	
КРТЕАМ	DALE	192.100.1.00					0	2012 R2	
Network Devices	DEXTER	192.710.1.102					0	2008 R2	
PNPL	DUCKTALES	192.100.1.100					0	Win 10	
SIEM1	ELC	192.110.1.77					0	Win 8.1	
SUPPORT	ESXVCSERVER	192.100.1.105					0	2003	
test123	ESXWIN2K12R2VM3	192.100.1.105					0	2012 R2	
TOONS	ESXWIN2K3R2VM3	192.100.1.170					0	2003	
VmWare	ESXWIN2K8R2VM1	192.100.1.200					0	2012 R2	
Win 7 and Server 2008 Above	ESXWIN2K8R2VM3	192.100.1.00					0	2008 R2	
Win XP and Server 2003	ESXWIN2K8R2VM7	192.100.111					0	2008 B2	

Figure: 3

- Select the system where you wish to install agent and Change audit.
- Click the checkbox under **Install Agent** and **Install CA** column.

**NOTE**: The change audit column will be displayed only for those users having the license for the same.

• Click Next.

CTION	COMPUTER LIKE							
install agent/Start poll 🔹			GO	All Agent 🗆 i	All Change Audit			Clea
		1			1	1		
Group Name	System name	IP Address	Agent version	Install Agent	CA version	Install CA	Port No	Device Type
al groups	RAGHEERA	192				<b>1</b>		Win III
ert foult	BUB CACOFONID	192.1				•	0	Win 10
omain Controllers	CASPER	192 100 1 113					0	Min 7
ventTracker		107 1					0	Win 7
irewall Devices	CINDERFILA	192.1					0	Will 7
PTEAM	DALE	192.100.1.03					0	2012 B2
vetwork Devices	DEXTER	192,100,1,71		Г			0	2008 R2
NPL	DUCKTALES	192.100.1.102					0	Win 10
EM1	ELC	192.100.1.100		Г			0	Win 8.1
JPPORT	ESXVCSERVER	192.100.1.77					0	2003
st123	ESXWIN2K12R2VM3	192.111.1115					0	2012 R2
ONS	ESXWIN2K3R2VM3	192.100.1.100					0	2003
1Ware	ESXWIN2K8R2VM1	192.1					0	2012 R2
n 7 and Server 2008 Above	ESXWIN2K8R2VM3	192.100.1.200					0	2008 R2
in XP and Server 2003	ESXWIN2K8R2VM7	192.100.100					0	2008 R2
	ESXWIN2K8VM1	192.100.1.107					0	2008
	ETSBI02	192.100.1.59					0	2012 R2
	FELDC	192.1.0.1.0.5					0	Win 7
	GENIE	192.111.1110					0	Win 10
	HERCULES	192.110.1.112					0	Win 10
	HUEY	192.110.1.00					0	Win 7
	LOUIE	192.100.100					0	Win 10
	1102	100 120 1 54			1			W8- 40



The Install Option window displays.

in options						
nstall Path						
%ProgramF	es%\Prism Micros	ystems				
• Agent ba	ed [full featured]			O Agent less (I	Limited featured	]
🗆 Inst	ll default Remedial	Action EXEs on this	system 🚺	Poll every	15 Minutes	-
🗹 Dep	DY SCAP		-			
🗹 Dep	ay WinSCP					
Apply con	guration					
After ev	nts are collected, t	hey are processed a	it the Manager			
To apply	a predefined confi	guration, select 'Cu	istom' and spe	cify the file.		
You car	also select 'Default	' and configure late	er.			
<ul> <li>Default</li> </ul>	O Custom confi	guration Select fi	le etaconfig.i	ni		Ŧ
						Install

**NOTE:** The **Deploy SCAP** and **Deploy WinSCP** options will be available only for licensed version.

• Check the 'Install default Remedial Action EXE on this system" option.

It will display a confirmation message box.



%ProgramFiles%\Prism Mi	crosystems			
Agent based [full feature	:d]	🔿 Agent less (	Limited featured]	
🔽 Install det <mark>Confirma</mark>	ation		× .	]
Deploy S(	<b>T C C C C C C C C C C</b>			-
☑ Deploy W	This reacure permits the execu Carefully review the risks and l feature. Are you sure?	tion of scripts on agent s benefits before enabling	this	
Apply configura		Ves	No	
After events a				
You can also select 'Def	ault' and configure later.	and specify the file.		
● Default 🛛 Custom c	onfiguration Select file eta	config.ini		Ŧ

- To use custom configuration, click the **Custom configuration** option and select the .ini file.
- Select **Yes** and then click the **Install** button.

It will request the user to authenticate using the windows security credential or the Smart card credentials.



	Windows Security X
To install a Please enter y	igent our credentials!
	User name Password Domain: PNPLVISTA
	Karen Smith Smart card credential
	OK Cancel

Figure: 7

• Select Smart Card credentials.

	Windows Security	x
To install a Please enter yo	gent our credentials!	
Ρ	Use another account	
	Karen Smith karen@pnplvista.test Smart card credential ÞIN Username hint	
	OK Cano	:el
	Figure: 8	



• Enter the smart card credentials and click **OK**.

The below message gets displayed.



- Click OK.
- To view the status of the installation, click the **Installation Status** in the Agent Utility window.

🎙 Agent Utility									_ 🗆 >
ACTION Install agent/Start poll			GO	All Agent 🗆 a	All Change Audit			Clea	Installation status r Refresh
Group Name	System name	IP Address	Agent version	Install Agent	CA version	Install CA	Port No	Device Type	-
All groups	BAGHEERA	192.168.1.134					0	Win 10	
Alert	вов	192.168.1.120				<b>v</b>	0	Win 10	
Default	CACOFONIX	192.168.1.158					0	XP Pro	
Domain Controllers	CASPER	192.168.1.113					0	Win 7	
EventTracker	CHIPDALE	192.168.1.81					0	Win 7	

Figure: 10

• The Installation Status can be viewed as shown below:

🎁 Installation st	atus					
Application		Status All		▼ Sort by	Date	•
Date	Svstem	Bv	Agent	Тире	Status	Description
8/29/2016 10:45	AM BOB	Toolioi 'i	Change Audit	Install agent	Success	Installed successfully.
8/29/2016 10:45	AM BOB	T221121	EventTracker	Install agent	Success	Installed successfully.
8/23/2016 6:33 F	PM PNPL-TESTLAB2	ougumeen	EventTracker	Uninstall agent/Stop poll	Success	Uninstallation done successfully.
8/23/2016 6:31 F	PM PNPL-TESTLAB2		EventTracker	Install agent	Success	Installed successfully.
8/23/2016 6:05 F	PM PNPL-TESTLAB2	8 <u></u>	EventTracker	Install agent	Success	Installed successfully.
8/23/2016 6:05 F	PM PNPL-TESTLAB2	ergennen -	Change Audit	Install agent	Success	Installed successfully.
8/19/2016 5:01 F	PM R1S4-VM1.Toons.local~Prism	shothan	EventTracker	Uninstall agent/Stop poll	Success	Uninstallation done successfully.



#### To upgrade an agent,

- In the Action field, select Upgrade from the dropdown list.
- Select the Group from the **Group Name** pane.

All the systems where agent needs to be upgraded will get listed.



- Select the system and check the options where you wish to upgrade the Agent/Change Audit
- Click Next.

ACTION       Upgrade       COMPUTER LIKE       Installation status         @       All Agent       All Agent       All Change Audit       Clear       Refresh         All groups	Agent Utility									
System nameIP AddressAgent versionUpgrade AgentCA versionUpgrade CAPort NoDevice TypeAll groupsMCLOON-II192,168.1.698,2 - Build 14II14505Vin 7DeraultSVR2012VM01192,168.1.2378,2 - Build 14II145052012 R2Domain ControllersEventTrackerFirewall DevicesNetwork DevicesPNPLPNPLSURPORTtest groupYmWareWin 7 and Server 2003 AboveWin 7 and Server 2003WORKGROUP	ACTION Upgrade	COMPUTER LIKE		60	🗆 All Agent 🗆 A	ll Change Audit			In: Clear	tallation status Refresh
Microws         Wicrows         Wicrows <t< th=""><th>Group Name</th><th>System name</th><th>IP Address</th><th>Agent version</th><th>Upgrade Agent</th><th>CA version</th><th>Upgrade CA</th><th>Port No</th><th>Device Type</th><th>4</th></t<>	Group Name	System name	IP Address	Agent version	Upgrade Agent	CA version	Upgrade CA	Port No	Device Type	4
Domain Controllers   EventTracker   Firewall Devices   Network Devices   PNPL   PRISM   SIEM1   SUPPORT   test group   TooNS   Win 7 and Server 2008 Above   Win XP and Server 2003   WORKGROUP	All groups Default	SVR2012VM01	192.168.1.69	8.2 - Build 14 8.2 - Build 14	<u> </u>	8.2 - Build 14		14505	Win / 2012 R2	
EventTracker   Firewall Devices   Network Devices   PNPL   PRISM   SIEM1   SUPPORT   text group   TOONS   VmWare   Win 7 and Server 2008 Above   Win XP and Server 2003   WORKGROUP	Domain Controllers		1	1	1	1	1	1	1	I
Firewall Devices   Network Devices   PNPL   PRISM   SUPPORT   test group   TooNS   Win 7a nd Server 2008 Above   Win XP and Server 2003   WORKGROUP	EventTracker									
Network Devices   PNPL   PRISM   SIEM1   SUPPORT   test group   TooNs   Win 7a and Server 2008 Above   Win XP and Server 2003   WORKGROUP	Firewall Devices									
PNPL   PRSM   SUPPORT   text group   TooNs   Win 7a and Server 2008 Above   Win XP and Server 2003   WORKGROUP	Network Devices									
PRISM   SEM1   SUPPORT   test group   TOONS   Win 7a and Server 2008 Above   Win XP and Server 2003   WORKGROUP	PNPL									
SEM1 SUPPORT test group TOONS VmWare Win 7 and Server 2008 Above Win XP and Server 2008 WorkGROUP	PRISM									
SUPPORT         test group         TOONS         Win 7 and Server 2008 Above         Win XP and Server 2008         Win XP and Server 2003         WORKGROUP	SIEM1									
test group TOONS WmWare Win 7 and Server 2008 Above Win XP and Server 2003 WORKGROUP	SUPPORT									
TOONS       VmWare       Win 7 and Server 2008 Above       Win XP and Server 2003       WORKGROUP	test group									
Vm/Ware       Win 7 and Server 2008 Above       Win XP and Server 2003       WORKGROUP	TOONS									
Win 7 and Server 2008 Above Win XP and Server 2003 WORKGROUP	VmWare									
Win XP and Server 2003 WORKGROUP	Win 7 and Server 2008 Above									
WORKGROUP	Win XP and Server 2003									
	WORKGROUP									
										NE×

Figure: 12

• Check the 'Install default Remedial Action EXE on this system" option.

It will display a confirmation message box.



%ProgramFiles%\F	rism Microsystems			
• Agent based [fu	ll featured]	O Agent le	ess [Limited featured]	
🗹 Install de	na char eve ur	. ^	·	]
Deploy §	philmation			
🗹 Deploy V	This feature permits the ex Carefully review the risks a feature. Are you sure?	ecution of scripts on age and benefits before enabli	nt systems. ng this	
Apply configur				
After events		Yes	No	
To apply a p				
You can also se	lect 'Default' and configure later.			
Default     O	ustom configuration Select file	etaconfig.ini		-



- To use custom configuration, click the **Custom configuration** option and select the .ini file.
- Select **Yes** and then click the **Upgrade** button.

It will request the user to authenticate using the windows security credential or the Smart card credentials.

• Select Smart Card credentials.



Windows Security	x
To install agent Please enter your credentials!	
Use another account	
Karen Smith         karen@pnplvista.test         Smart card credential         PIN         Username hint	
OK Cano	:el

Figure: 14

• Enter the smart card credentials and click **OK**.

The below message gets displayed.



Figure: 15

- Click **OK**.
- The Installation Status can be viewed as shown below:



Installation statu	5						×
Application All		•	Status Al	l	•	Sort by Date	
Date	System	Ву	Agent	Туре	Status	Description	
8/29/2016 6:37 PM	MCLOON-II	TTTTTT	EventTracker	Upgrade agent	Success	Upgrade done successfully.	
8/29/2016 6:37 PM	MCLOON-II	toono lii	Change Audit	Upgrade agent	Success	Upgrade done successfully.	



#### To uninstall an agent,

- In the Action field, select Uninstall agent/Stop poll from the dropdown list.
- Select the Group from the **Group Name** pane.

All the systems where agent can be uninstalled get listed.

- Select the system and check the options (Agent/Change Audit) which you wish to uninstall.
- Click Next.

Agent Utility									
ACTION Uninstall agent/Stop poll	COMPUTER LIKE		GO	🗆 All Agent 🗆 Al	ll Change Audit			Ins Clear	tallation status Refresh
Group Name	System name	IP Address	Agent version	Uninstall Agent	CA version	Uninstall CA	Port No	Device Type	
All groups	MCLOON-II	192.168.1.69	8.2 - Build 14		8.2 - Build 14		14505	Win 7	
Default	SVR2012VM01	192.168.1.237	8.2 - Build 14				14505	2012 R2	
Domain Controllers									-
EventTracker									
Firewall Devices									
Network Devices									
PNPL									
PRISM									
SIEM1									
SUPPORT									
test group									
TOONS									
VmWare									
Win 7 and Server 2008 Above									
Win XP and Server 2003									
WORKGROUP									
	_								
									NEX

Figure: 17

It will request the user to authenticate using the windows security credential or the Smart card credentials.



• Select Smart Card credentials.

	Windows Security X
To install a Please enter y	gent our credentials!
Р	Use another account
	Karen Smith karen@pnplvista.test Smart card credential PIN Username hint
	OK Cancel

Figure: 18

• Enter the smart card credentials and click **OK**.

The below message gets displayed.



- Click OK.
- The Installation Status can be viewed as shown below:

	Installation status							2
	Application All	•	Sta	itus All	•	Sort by	Date	
	Date	System	Ву	Agent	Туре	Status	Description	
E	8/30/2016 11:23 AM	SVR2012VM01	100101	EventTracker	Uninstall agent/Stop poll	Success	Uninstallation done successfully.	
	8/29/2016 6:37 PM	MCLOON-II	T00000	EventTracker	Upgrade agent	Success	Upgrade done successfully.	
	8/29/2016 6:37 PM	MCLOON-II	TOONG 'I	Change Audit	Upgrade agent	Success	Upgrade done successfully.	





\*\* **IMPORTANT NOTE:** If the user gets an error displaying '**Copying files to the remote system failed**" in the Installation status, as shown in the figure, follow the steps mentioned below:

Installation status										
Application all	×		Statue	Al	*	Surlay	Cale	*	Rates	
Cale	Europe	By	Acquire	Tapa	Tistu	Custophin				
9/14/2016 4:55 PM	PHPL TESTLADS	sunanda	EventTracker	Install agent	Failed	Copying files to	o the remote sys	tem failed.		
STACOT ASARTH	geoglicesetians!	ouroandla	N/6.	Search-computers	Thereise	Second was in	arran Ral			
5/30./3076-0.34 PM	192 168 1 52	shallondka	16/4	Search computers	Sine					
5/08/0016 @ 32/PM	RITESVINIT	distinguitor.	N/A	Taxath computers	Thissue.					
\$/01/2016-8:31 PM	1132 1988 1 52	distinction.	16/4A	Seath corganes	Thistory .					
S/SIL/SISHE & ST PM	1952 1968 1 52	distinguistics.	19/44	Tenach-computers	-					

Figure: 21

- 1. Check the log '**Remins.txt**" in the Install Directory\EventTracker\RemoteInstaller folder.
- 2. If the log consists of the **Error:-2146434964**, the user will have to log off the system and log in again with the Smart card credentials and then try deploying the agents.

