

Exgarde SIMONSVOSS INTEGRATION

User Guide UM0085.GB Issue 3 23/07/2015

www.tdsi.co.uk

TDSi Unit 10 Concept Park Innovation Close Poole Dorset BH12 4QT, UK Tel: +44 (0) 1202 723535 Fax: +44 (0) 1202 724975

Sales Enquiries: Marketing Support: Technical Support: sales@tdsi.co.uk marketing@tdsi.co.uk support@tdsi.co.uk

Foreword

Copy right © 2015 TDSi. All rights reserved.

Time and Data Systems International Ltd operate a policy of continuous improvement and reserves the right to change specifications, colours or prices of any of its products without prior notice.

Guarantee

For terms of guarantee, please contact your supplier.

Trademarks

Copyright © 2015 Time and Data Systems International Ltd (TDSi). This document or any software supplied with it may not be used for any purpose other than that for which it is supplied nor shall any part of it be reproduced without the prior written consent of TDSi.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other brands and product names are trademarks or registered trademarks of their respective owners.

Cautions and Notes

The following symbols are used in this guide:



CAUTION! This indicates an important operating instruction that should be followed to avoid any potential damage to hardware or property, loss of data, or personal injury.



NOTE. This indicates important information to help you make the best use of this product.

Contents

1.	Overview	.1
2.	Getting Started	.2
З.	IP Lock Service Manager	.3
4.	Firewall Configurations	.5
5.	Configuring EXgarde	.10
6.	Configuring Doors	.12
7.	White List	.13
8.	Office Mode	.16



1. Overview

EXgarde provides the ability to integrate with Simon Voss IP locks by connecting to the SimonsVoss Wave Net Radio network. The EXgarde interaction includes controlling and monitoring locks and because EXgarde connects to the Wave net hub, with each hub handling 16 locks, the only limitations to this service is hardware capability and the IP lock license.



2. Getting Started

Before EXgarde can integrate with SimonsVoss IP locks, you will need to ensure the SimonsVoss locks and hubs have been installed and set up correctly prior to setup in EXgarde. Please refer to the SimonsVoss Installation Guide for further information. The IP Lock Service manager will also need to be installed prior to configuring the IP locks.

The following information will need to be obtained from the SimonsVoss application.

- Unit Number This will be the last 3 digits of the GN device address
- Door Number This will be the last 3 digits of the LN device address
- Connection details This will be the IP address for the Hub
- PHI String This is the door locks unique ID. It can also be found etched on to the lock body





3. IP Lock Service Manager

To enable communications between EXgarde and the IP Locks communication hub, the IP Lock Service must be running. The Service Manager can be used to configure the IP Locks Service. This can be found in C:\Program Files\TDSi\Exgarde\IPLocks\IPLockServiceManager.exe.

Organize 🔻 💼 Open 🛛 New folder					⊞ ▼	0
👉 Favorites	Name	Date modified	Туре	Size		
Downloads	Exgarde.ExgardeSettings.dll	29/04/2014 15:05	Application extens	6 KB		
Recent Places	Exgarde.ExgardeSettings.pdb	29/04/2014 15:05	PDB File	14 KB		
and recent races	EXgarde.Localization.dll	29/04/2014 15:05	Application extens	147 KB		
🗃 Libraries	EXgarde.Localization.pdb	29/04/2014 15:05	PDB File	194 KB		
	Exgarde.pdb	29/04/2014 15:05	PDB File	72 KB		
📮 Computer	EXgarde.TCM.dll	29/04/2014 15:05	Application extens	15 KB		
T. compare	EXgarde.TCM.pdb	29/04/2014 15:05	PDB File	32 KB		
🗣 Network	🚳 ExgardeDataDomain.dll	29/04/2014 15:05	Application extens	35 KB		
T. HERROR	ExgardeDataDomain.pdb	29/04/2014 15:05	PDB File	14 KB		
	ExgardeDataLayer.dll	29/04/2014 15:05	Application extens	41 KB		
	ExgardeDataLayer.pdb	29/04/2014 15:05	PDB File	58 KB		
	ExgardeObjects.dll	29/04/2014 15:05	Application extens	12 KB		
	ExgardeObjects.pdb	29/04/2014 15:05	PDB File	24 KB		
	IPCommunications.dll	29/04/2014 15:05	Application extens	19 KB		
	IPCommunications.pdb	29/04/2014 15:05	PDB File	46 KB		
	IPLockServiceManager.exe	21/01/2014 13:42	Application	11 KB		
	IPLockServiceManager.pdb	21/01/2014 13:42	PDB File	22 KB		
	IPLocksService.exe	29/04/2014 15:05	Application	23 KB		
	IPLocksService.exe.config	29/04/2014 16:46	CONFIG File	3 KB		
	IPLocksService.pdb	29/04/2014 15:05	PDB File	38 KB		
	IPLocksService.vshost.exe	29/04/2014 15:04	Application	23 KB		
	IPLocksService.vshost.exe.config	29/04/2014 16:46	CONFIG File	3 KB		
	IPLocksService.vshost.exe.manifest	06/06/2012 02:06	MANIFEST File	1 KB		
	NLog.config	14/01/2014 16:27	CONFIG File	1 KB		
	🚳 NLog.dll	15/10/2013 08:50	Application extens	430 KB		
	📄 NLog.xml	15/10/2013 08:50	XML Document	750 KB		
	🚳 ReaderModes.dll	29/04/2014 15:05	Application extens	7 KB		
	ReaderModes.pdb	29/04/2014 15:05	PDB File	22 KB		
	🚳 Topshelf.dll	26/09/2013 15:36	Application extens	236 KB		

The Lock Service Manager can be used to control/configure the IP Lock Service; the start/stop buttons can be used to start or stop the service. When you first run EXgarde, the IPLocksService will be set to run in manual mode by default. This can be changed to run in Automatic mode by right clicking on the shortcut you have just created and selecting Run as administrator, click yes on the next screen to accept running as Administrator. The IP Lock Service Manager will open and 'Start-up type' will default to Manual. To enable Automatic start-up of the service, click Stop then Uninstall, then select Automatic from the drop down list and click Install, next click on Start. From now on every time the PC running EXgarde is started the IP Service will start.

ock Service Manage	er 🗾	3
Startup type Automatic	•	
Install	Uninstall	
Start	Stop	
	Startup type Automatic Install	Startup type Automatic - Install Uninstall

To check if the service is running and has been changed to automatic start, go to Services and the IP Locks Service Manager status and Start up Type should be the same as shown in the screenshot below. Status should be started and Startup Type should be Automatic

• 🔿 🔲 🔄 🦉	G 🕞 🔽 📰 🕨 🔳 🕪						
Services (Local)	Services (Local)						
	Exgarde IP Locks	Name	Description	Status	Startup Type	Log On As	
		😪 Exgarde IP Locks	Exgarde IP Lock Integration	Started	Automatic	Local Syste	ſ
	Stop the service Restart the service	Extensible Authentication Protocol Extour TCM Service	The Extensible Authentication Protocol (EAP) servi Extour TCM Service	Started	Manual Automatic	Local Syste Local Syste	
		💁 Fax	Enables you to send and receive faxes, utilizing fax		Manual	Network S	
	Description:	Function Discovery Provider Host	The FDPHOST service hosts the Function Discover		Manual	Local Service	
	Exgarde IP Lock Integration	Function Discovery Resource Publ	Publishes this computer and resources attached to	Started	Automatic	Local Service	
		🔍 Group Policy Client	The service is responsible for applying settings co	Started	Automatic	Local Syste	
		🔍 Health Key and Certificate Manag	Provides X.509 certificate and key management se		Manual	Local Syste	
		🧠 HomeGroup Listener	Makes local computer changes associated with co		Manual	Local Syste	
		🔍 HomeGroup Provider	Performs networking tasks associated with config		Manual	Local Service	
		🧠 Human Interface Device Access	Enables generic input access to Human Interface		Manual	Local Syste	
		🔍 IKE and AuthIP IPsec Keying Mod	The IKED(T service hosts the Internet Key Exchang		Manual	Local Syste	
		Interactive Services Detection	Enables user notification of user input for interacti		Manual	Local Syste	
		🔍 Internet Connection Sharing (ICS)	Provides network address translation, addressing,		Disabled	Local Syste	
		🔍 IP Helper	Provides tunnel connectivity using IPv6 transition	Started	Automatic	Local Syste	
		🔍 IPsec Policy Agent	Internet Protocol security (IPsec) supports network	Started	Manual	Network S	
		🔍 KtmRm for Distributed Transactio	Coordinates transactions between the Distributed		Manual	Network S	
		🔍 Link-Layer Topology Discovery M	Creates a Network Map, consisting of PC and devi		Manual	Local Service	
		Microsoft .NET Framework NGEN	Microsoft .NET Framework NGEN		Manual	Local Syste	
		🔍 Microsoft .NET Framework NGEN	Microsoft .NET Framework NGEN		Automatic (D	Local Syste	
		Microsoft iSCSI Initiator Service	Manages Internet SCSI (iSCSI) sessions from this c		Manual	Local Syste	
		🔍 Microsoft Software Shadow Copy	Manages software-based volume shadow copies t		Manual	Local Syste	
		🔍 Multimedia Class Scheduler	Enables relative prioritization of work based on sys	Started	Automatic	Local Syste	
		🔍 Net.Msmq Listener Adapter	Receives activation requests over the net.msmq an		Disabled	Network S	
		🔍 Net.Pipe Listener Adapter	Receives activation requests over the net.pipe prot		Disabled	Local Service	
		Net.Tcp Listener Adapter	Receives activation requests over the net.tcp proto		Disabled	Local Service	
		Net.Tcp Port Sharing Service	Provides ability to share TCP ports over the net.tcp		Disabled	Local Service	
		🔍 Netlogon	Maintains a secure channel between this compute		Manual	Local Syste	



4. Firewall Configurations

The default IP ports on the PC EXgarde has been installed on will be blocked by Windows Firewall. The following steps need to be carried out for both inbound and outbound rules

Search and open Windows Firewall with Advanced Security



Select Inbound Rules from the left window and then select New Rule in the Actions window on the right to start the wizard

Eile Action View Help			
Þ 🔿 🙋 📰 🗟 🛛 🗊			
Windows Firewall with Advanc	Inbound Rules		Actions
🗱 Inbound Rules 戳 Outbound Rules	Name	Group	Inbound Rules
Connection Security Rules	BranchCache Content Retrieval (HTTP-In) BranchCache Hosted Cache Server (HTT	BranchCache BranchCache	Vew Rule
Montoning	BranchCache Peer Discovery (WSD-In)	BranchCache Connect to a	Filter by State
	Connect to a Network Projector (TCP-In) Connect to a Network Projector (TCP-In)	Connect to a	Filter by Group
	Connect to a Network Projector (WSD Ev		View
	Connect to a Network Projector (WSD Ev	Connect to a	Refresh
	Connect to a Network Projector (WSD Ev Connect to a Network Projector (WSD-In)	Connect to a Connect to a	Help
	Ocore Networking - Destination Unreacha		-
	Ore Networking - Destination Unreacha Core Networking - Dynamic Host Config		
	Ocore Networking - Dynamic Host Config		
	Ore Networking - Internet Group Mana Core Networking - IPHTTPS (TCP-In)	Core Networ Core Networ	
	Core Networking - IPv6 (IPv6-In)	Core Networ	
	Ore Networking - Multicast Listener Do Core Networking - Multicast Listener Qu		
	Core Networking - Multicast Listener Rep		
	Core Networking - Neighbor Discovery A		

When the Rule Type window opens, select Port and click next

🔗 New Inbound Rule Wizard	
Rule Type	
Select the type of firewall rule to	create.
Steps:	What type of rule would you like to create?
 Rule Type Protocol and Ports Action Profile Name 	 Program Rule that controls connections for a program. Port Rule that controls connections for a TCP or UDP port.
	 Prgdefined: BranchCache - Content Retrieval (Uses HTTP) * Rule that controls connections for a Windows experience. Custom Custom rule.

From the Protocol and Ports window, select TCP and in Specific local port enter 2101 or specified IP port if changed from default then select next

🔗 New Inbound Rule Wizard					
Protocol and Ports					
Specify the protocols and ports to) which this rule applies.				
Steps:					
Bule Type	Does this rule apply to TCP or UDP?				
Protocol and Ports	© TCP				
Action	O UDP				
Profile					
Name	Does this rule apply to all local ports or specific local ports?				
	All local ports				
	Specific local ports:	2101			
		Example: 80, 443, 5000-5010			
	Learn more about protocol and pr				
		< <u>B</u> ack <u>N</u> ext > Cancel			

Select Allow the connection from the Actions window and click next

🔗 New Inbound Rule Wizard	
Action	
Specify the action to be taken w	hen a connection matches the conditions specified in the rule.
Steps:	
Rule Type	What action should be taken when a connection matches the specified conditions?
 Protocol and Ports Action 	Allow the connection
 Profile 	This includes connections that are protected with IPsec as well as those are not. Allow the connection if it is secure
• Name	This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Customize Block the connection
	Learn more about actions Kext > Cancel

If you are unsure which of the Profiles need to be selected in the Profile window contact your IT support.

🔗 New Inbound Rule Wizar	d 🖂
Profile	
Specify the profiles for which th	iis rule applies.
Steps:	
Rule Type	When does this rule apply?
Protocol and Ports	
Action	Domain
Profile	Applies when a computer is connected to its corporate domain.
Name	
	Applies when a computer is connected to a private network location.
	Public
	Applies when a computer is connected to a public network location.
	Leam more about profiles
	Cean more about promes
	<u>Back</u> Cancel

Finally, enter the name for the new rule and description if you desire and click Finish to complete the wizard.

🔗 New Inbound Rule Wizard		×
Name		
Specify the name and description of	of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action	Name:	
Profile	IP Locks Portal	
Name		
	Description (optional):	
	< <u>B</u> ack <u>Finish</u> Cano	cel

You can check the new Inbound rule by re-opening the Windows Firewall and Advanced Security window.

ile Action View Help			
Windows Firewall with Advance	Inbound Rules		Actions
Subound Rules Cutbound Rules Connection Security Rules Monitoring	Name V IP Locks Portal BranchCache Content Retrieval (HTTP-In) BranchCache Postel Cache Server (HTT BranchCache Peer Discovery (WSD-In) Connect to a Network Projector (TCP-In) Connect to a Network Projector (TCP-In) Connect to a Network Projector (WSD Ev Connect to a Network Projector (WSD In) Connect to a Network Projector (WSD In) Core Networking - Destination Unreacha Core Networking - Dynamic Host Config Core Networking - Internet Group Mana Core Networking - Multicast Listener Do Core Networking - Multicast Listener Qu Core Networking - Multicast Listener Qu	Connect to a Connect to a Connect to a Connect to a Connect to a Connect to a Connect to a Cone Networ Core Networ	Inbound Rules Kew Rule Kew Rule Kew Rule Kew Rule Kew Rule Kew Rule. Kew Rule Refresh Kew Refresh Kew Rule Rule Rule Kew Rule Rule Rule Kew Rule Rule Rule Rule Rule Rule Rule Rule
4	Core Networking - Multicast Listener Rep	Core Networ +	



5. Configuring EXgarde

To ensure the IP locks will work correctly, check the license server has been upgraded

👼 EXgarde License Server			
Eile			
Status information Connected Cli Product Licence Key Present Maximum Network Users Maximum Doors Maximum Tenants Database status Deleting Events IP Locks	ents EXgarde Enterprise Version : 4.4.0. Yes 100 800 10 Online Inactive 32	Licensed options Photo ID Fusion MICR0garde EXtour Elevator Control EXvisitor EXvisitor EXvisitor EXvisitor Zone APB Web	↓ F Upgrade
	Copyright (c) 1996 TDSi All rights reserved		E xit

Open EXgarde and create a new portal for the IP locks. Rename the portal and change the Type to IP locks. Then select SimonsVoss from the Lock Type menu. The default IP port is set to 2101.

N.B. IP port 2101 may be blocked by Windows firewall, if this is the case you will have to create a new inbound rule this is covered in Firewall Config

🎯 New	💾 Save	🗶 Delete	🥖 Properties	🕖 Events	*
N	Name SimonsVo	ss			
- Informa	ation				
Long	Name		Comment		
. Туре о	f Portal				
Туре		(Computer		
IP loc	:ks	•	TDSI-WIN7DEV4	•	
- Portal (Configuration Type	1			
Simor	ns Voss		•		
IP Add 127 .	lress 0.0.	1	IP Port 2101		
🗖 Se	cure Connec	ction			

Next you will need to create the ACU which represents the Hub. In Summary view click on <ACU> and click the drop down list on the New tab and choose SimonsVoss.



When adding the new ACU you will need to specify the Unit number and IP address. Please see your SimonsVoss software to obtain this information.

Name Simone Voes		Name	Long Name	Comment	Unit Numbe
Name Simons Voss Commission Mode Information Long Name Comment		🗆 🖭 aperio			0
		🗆 🖭 EXcel4			1
		🗆 🖭 EXpander			2
		🗆 🖭 EXpert2			2
		🗆 🖭 MICROgarde 1			5
Site		🗹 🖭 Simons Voss			100
Site 1	•				
- Communications					
Communication Portal					
TDSI-WIN7DEV4 : SV	•				
Configuration	_				
ACU Type	Default Configuration				
Simons Voss	DR 💌				
UID	Unit Number				
	000100				
Password	Auxiliary I/O Board				
мини	Not installed 💌				
Additional Configuration					
IP Comms Events	Holidays APB				

ACU Type will be greyed out and show as SimonsVoss. Click save when you have finished.



6. Configuring Doors

In Outline view the 16 doors belonging to the SimonsVoss will be shown directly below the new ACU you have created. If you click on any of the doors the door list will appear in the general display area in the right hand screen.

Left click on the relevant door in the list and select Properties,

You will need to assign a PHI string and the Door Number taken from the SimonsVoss software for the lock to operate correctly.

You can also set the Outer & Inner area. The Outer area being the area you are going from and the Inner Area being the area you are entering into to.

Any unused doors can be disabled by un-ticking the Enabled option in the Properties window



When you are satisfied with the information added click Save. You will need to repeat the configuring doors process to when adding a new door.



7. White List

The white list is a list made up of specified Keyholders and their key number. The list can be downloaded to each lock to ensure that if the IP lock service is disconnected or the server goes down, the specified Keyholders will still have access.

To create a White list, ensure the SimonsVoss IP locks are installed and operational.

The First step is to open the Access Tab under Keyholders.

Actions
🔚 Instant Report
🇞 Keyholders 🛛 🔝 Keys
Access Groups 💷 Badge Designs

Click on the New tab to create a new group and label it appropriately.

🎯 New 🔻 💾 Save 🗶 Delete	: 📝 Properties 🛛 👫 Schedule		
Name SV White List			
- Information			
Long Name Co	Comment		
 Configuration 			
Access Group Schedule 🛛 🗖	Include In White List		
Unrestricted Access 🔄 🗖	Intruder System Users		
- Lists			
Access Areas Keyholders			
Access Area			
🗹 Ŗ Public			
🗆 Ŗ Boardroom 1			
🗆 Ŗ Building			
🗆 📊 Canteen			
🗆 🙀 Car park			
🗆 🙀 Development			
🗆 🗛 П Dept			
🗆 👧 Lab			
🗆 🗖 Office			
Reception			
🗆 Ŗ Sales			

In the new group configuration, there is a check box to 'Include In White List'. This check box will ensure any Keyholders are sent to the locks.

Access Group Schedule	🔽 Include In White List
Unrestricted Access	🔲 🥅 Intruder System Users

You can then specify which Access Areas this new group will have access to.

Access	Areas	Keyho	lders	
Ac	cess Area			
🗹 🛐 Pul	blic			
	ardroom 1			
🗹 🖪 Bui	Iding			
🗆 🗖 Car	🙀 Canteen			
🗹 🗖 Car	r park			
🗆 🖪 De	R Development			
	Dept			
🗹 🖪 Lab				
🗆 🖪 Off	Office			
🗆 🖪 Red	eption			
🗆 📕 Sal				

You can also specify which Keyholders will be included in the white list by selecting the Keyholders from the Keyholders tab.

Access Areas Keyholders	
Name	Tenant
檺 Keyholder 1	Landlord
檺 Keyholder 2	Landlord
檺 Keyholder 3	Landlord
🗽 Keyholder 4	Landlord
🛿 🍖 Keyholder 5	Landlord
檺 Keyholder 6	Landlord
🍇 Keyholder 3	Landlord
檺 Keyholder 4	Landlord
檺 Keyholder 5	Landlord
🍇 Keyholder 6	Landlord
🍇 Keyholder 7	Landlord
🗽 Keyholder 8	Landlord
🍇 Keyholder 9	Landlord
💑 Keyholder 10	Landlord
	لتناج المحتم ا

When you have completed the setup, click on Save. This will prompt your to refresh the ACU's in the system.

To ensure the White list is sent to the SimonsVoss readers. Go to the Equipment Tab and select the SimonsVoss ACU.

Then select the 'Send all valid Keys to ACU' from the Actions Menu.

Actions	
🔿 Send configuration and Keys to ACU 🚽	
🛠 Send configuration to ACU	
Send all valid Keys to ACU	Ξ
뒏 Dial Remote ACU	
💿 Show events	
🕒 Show Alarms	-
🔑 Calculate Key usage in ACU	
🚪 Update equipment states	
📃 Suspend	Ŧ
< III	

This will complete the process.



8. Office Mode

One of the key feature EXgarde and SimonsVoss can perform is the ability to operate an office mode on any of functioning locks. Office mode allows a Trustee to permanently unlock a reader with 2 or more presentation of their card. This feature is particularly useful if do not want to issue cards but still would like non card holders to access and area I.E a training room.

To set up office mode, you will need to enable the Multi-card function, establish trustees and apply the office mode to the required locks.

To enable the Multi-card Access Support function, click on the system setting button and navigate to the options tab.

Schedules 🚺 Database Users 🕌 Operators
🛠 Options 😅 Netcam type list
Active Tenant: Landlord
-
Keyholders
Equipment
Reports
Building Management
System Settings
Tenants

Within the System Option menu is Compatibility. This option will allow to enable Multi-card Access Control Units. Ensure this has been selected before you save and exit.

💼 New 📃 Save 🗶 Delete	
	Options
System Option	🛠 About EXgarde
	🛠 Event Log Control
	🛠 Compatibility
	🛠 Area Bookings
	X Occupancy
	🛠 Keypad-only Digits
EXseries Access Control Units	🛠 Universal Decode
	K Enrolment Readers
64 🖨 Maximum number of Group Schedules	🛠 Biometric Enrolment
<u>,</u>	🛠 Reader Types
Multi-card Access Support	🛠 Update Statistics
Disable Events	🛠 Video Verfication Opti
	🛠 Dual Login
	🛠 Wizard Defaults

Next you will need to set up a trustee, to do this open the properties tab on the desired Keyholder and select the Trustee radial button.

🔆 New 🔻 🗖 Save 🗶	Delete 🔻 <u>/</u> Properties	Jean Sear
💿 Show events 🛛 🙀 Keyh	older access 🛛 🗼 Export Key	holders
*		
Name New Keyholder 1		
 Keyholder Information 		
Long Name	Comment	
1		
 Keyholder Keys 		
	Туре	
Keyholder Keys Key to issue	Type Microcard	•
Key to issue	 Microcard 	•
Key to issue	Microcard	•
Key to issue	Microcard Access Group	•
Key to issue Keyholder Security Options Keyholder Trustee	Microcard Access Group All	•
Key to issue Keyholder Security Options Keyholder Trustee Trackable		
Key to issue Keyholder Security Options Keyholder Trustee	Microcard Access Group All	

Click save when complete.

The final step is to enable office mode on the desired lock. To do this select the relevant reader or readers from the equipment list and select the properties tab.



Select the Multi-card tab and select Office Mode from the Multi-card Access Mode drop down menu.

Additional		
Multi-card	Events	
Multi-card Acce	ess Mode	
Office Mode	-	
Off Office Mode		
		Timeout
2		10 🗎

To complete the process, click the Save button

Time and Data Systems International Ltd Unit 10 Concept Park Innovation Close Poole Dorset BH12 4QT UK

+44 (0)1202 723535 +44 (0)1202 724975

http://www.tdsi.co.uk/ sales@tdsi.co.uk marketing@tdsi.co.uk support@tdsi.co.uk