



Radio Dispatch Engineering Group

IP-30XX Hardware Console Administrator Guide



Revision B

March 11, 2021



Table of Contents

1.	Re	vision History	.1
2.	Re	quired Equipment	.1
3.	Ov	erview	. 1
4.	Ga	ining Administrator Access	. 1
4 4	.1 .2	Logging in as Admin Accessing the Desktop Enabling ping	. 1 . 1
4	.3	Enabling ping	. 2



1. Revision History

Revision	Date	Author	Description
A	03/04/2021	Radio Dispatch Engineering Group	Initial Release
В	03/11/2021	Radio Dispatch Engineering Group	Enabling ping updated

2. Required Equipment

IP-30XX Console

3. Overview

The purpose of this document is to give instructions to IT administrators that need to make changes to the IP-30XX underlying Operating System. It will show how to access the administrator account, access the desktop of the OS, as well as enable pinging in the firewall.

4. Gaining Administrator Access

4.1 Logging in as Admin

- 1. Press Ctrl-Alt-Del
- 2. Select Log Off
- 3. Select DispatchAdmin Account
- 4. Enter password(default is telex)
- 5. Windows will require you to change password

4.2 Accessing the Desktop

- 1. After logging in as DispatchAdmin press Ctrl-Alt-Del
- 2. Select Task Manager
- 3. Select File -> Run new task

N	😰 Task Manager							
File	ile Options View							
	Run new task	pp history	Startup	Users	Detai	ls Service	25	
	Exit			~ 5	201			
		-		1 2	32%			
Name					CPU	Status		

- 4. Enter explorer.exe
- 5. Check Create this task with administrative privileges



🖅 Crea	Create new task						
i.	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.						
<u>O</u> pen:	explorer.exe ~]					
	OK Cancel <u>B</u> rowse						

- 6. Select OK
- 7. Windows Desktop is now shown and windows can be used as normal Note: Start Menu is still disabled in this mode.

5. Enabling ping

- 1. Press Windows Key-R
- 2. Enter gpedit.msc and select OK

📨 Run	×
0	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	gpedit.msc ~
	OK Cancel <u>B</u> rowse



IP-30XX Administrator Guide

le <u>A</u> ction <u>V</u> iew <u>H</u> elp		
• 🔿 🚈 💼 🛃 🗊		
Local Computer Policy	Name	Group
👰 Computer Configuration		1. (A)
> 📔 Software Settings	There are	no items to show in this view.
🗸 🚞 Windows Settings		
> 🧾 Name Resolution Policy		
😫 Scripts (Startup/Shutdown)		
> 📾 Deployed Printers		
🗸 🚡 Security Settings		
> 📴 Account Policies		
> 📴 Local Policies		
🗸 🚞 Windows Defender Firewall with Advanced Security		
🗸 🎡 Windows Defender Firewall with Advanced Security - Local Group Policy Object		
🗱 Inbound Rules		
🗱 Outbound Rules		
🌆 Connection Security Rules		
🛅 Network List Manager Policies		
> 🛅 Public Key Policies		
> 📔 Software Restriction Policies		
> Application Control Policies		
🔉 뢿 IP Security Policies on Local Computer		
> Advanced Audit Policy Configuration		
> policy-based QoS		
> 🚰 Administrative Templates		
% User Configuration		
> 📔 Software Settings		
> 📔 Windows Settings		
> 🛗 Administrative Templates	<	

- 3. Navigate to: Local Computer Policy/Computer Configuration/Windows Settings/Security Settings/Windows Defender Firewall with Advanced Security/Windows Defender Firewall with Advanced Security – Local Group Policy Object/Inbound Rules
- 4. Right click Inbound Rules->New Rule...



🎡 New Inbound Rule Wiza	ard	×
Rule Type Select the type of firewall rule to	o create.	
Steps: Rule Type Program Protocol and Ports Scope Action Profile Name	What type of rule would you like to create? Porgram Rule that controls connections for a program. Pot Rule that controls connections for a TCP or UDP port. Predefined: @FirewallAP1.dll_80200 Rule that controls connections for a Windows experience. @ Lestom Custom rule.	8

5. For the Rule Type enable Custom radio button and select Next



💣 New Inbound Rule Wizard		×
Program Specify the full program path and	executable name of the program that this rule matches.	
Steps: Rule Type Program Protocol and Ports Scope Action Profile Name	Opes this rule apply to all programs or a specific program? • All programs Rule applies to all connections on the computer that match other rule properties. • Ihis program path:	

6. For the Program enable All programs radio button and select Next



📸 New Inbound Rule Wiza	rd				×
Protocol and Ports Specify the protocols and ports to	to which this rule applies.				
Steps: Rule Type Program	To which ports and p	rotocols does this ru	le apply?		
 Protocol and Ports Scope Action Profile 	Protocol type: Protocol n <u>u</u> mber:	ICMPv4		~	
 Prome Name 	Local port: <u>R</u> emote port:	All Ports Example: 80, 4 All Ports	143, 5000-5010	~	
	Internet Control Mess (ICMP) settings:		143, 5000-5010 <u>C</u> ustomize.		
				Deal Marks	Const
			< 1	<u>B</u> ack <u>N</u> ext >	Cancel

7. For the Protocol and Ports select Protocol type->ICMPv4 and select Customize

IP-30XX Administrator Guide



Customize ICMP Settings	×
Apply this rule to the following Internet Control Message Protocol (ICMP) connections:	
<u>A</u> II ICMP types	
○ Specific ICMP types	
 Packet Too Big Destination Unreachable Source Quench Redirect Echo Request Router Advertisement Router Solicitation Time Exceeded Parameter Problem Timestamp Request Address Mask Request 	
This ICMP type:	
Type: 0 V Code: Any V Add	
OK Cancel	

8. For the Customize ICMP Settings enable All ICMP types radio button and select OK



New Inbound Rule Wiza Scope	rd	>
	addresses to which this rule applies.	
Steps: Rule Type Program Protocol and Ports Scope	Which local IP addresses does this rule apply to? Any IP address In these IP addresses:	
 Action Profile Name 	Customize the interface types to which this rule applies: Which remote IP addresses does this rule apply to? Any IP address These IP addresses:	Add Edit Remove
	< <u>B</u> ack	Add Edit Remove

9. For the Scope enable Any IP address radio buttons and select Next



🍻 New Inbound Rule Wiza	ard	×
Action Specify the action to be taken	when a connection matches the conditions specified in the rule.	
Steps: Rule Type Program Protocol and Ports Scope Action Profile Name	What action should be taken when a connection matches the specified conditions? Image: Contract Cont	

10. For the Action enable Allow the connection radio button and select Next



🔐 New Inbound Rule Wizard X			
Profile			
Specify the profiles for which th	s rule applies.		
Steps:	When does this rule apply?		
 Rule Type Program 	when does this fulle apply ?		
 Protocol and Ports Scope Action 	 Domain Applies when a computer is connected to its corporate domain. Private 		
Profile	Applies when a computer is connected to a private network location, such as a home or work place.		
Name	Public Applies when a computer is connected to a public network location.		
	< Back Next > Cancel		

11. For the Profile enable the Profiles to apply the rule and select Next



IP-30XX Administrator Guide

🔐 New Inbound Rule Wizard		×
Name Specify the name and description of	this rule.	
Steps: Rule Type Program Protocol and Ports Scope Action Profile Name	Name: ICMP v4 Description (optional): Enable Ping	ncel

12. For the Name enter a Name and Description and select Finish