



रक्षा लेखा नियंत्रक का कार्यालय, गुवाहाटी उदयन विहार, नारंगी, गुवाहाटी-781171

OFFICE OF THE CONTROLLER OF DEFENCE ACCOUNTS

UDAYAN VIHAR, NARANGI, GUWAHATI: 781171.

ई-मेल/e-mail:cda-guw@.nic.in फेक्स/FAX:0361-2640204 फोन/Ph: 0361-2640394, 2641142.

विकसित भारत
अभियान
1947-2024

No. CDA GUW/IT&SW/1304/CYBER-SECURITY/2025

Date -29/07/2025

Circular No: -95

To
The Officer In-charge
All Sub-Offices
All sections (Local)

Subject: - Advisories on WAN Security – Action thereon.

Reference: - HQrs Letter No. IT&S/806/WAN Security/2024-25 dated 23/06/2025.

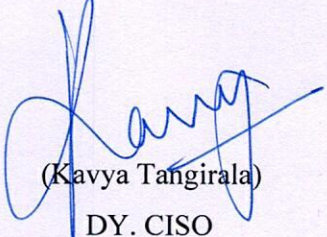
HQrs office vide letter cited above has issued critical advisories on WAN security.

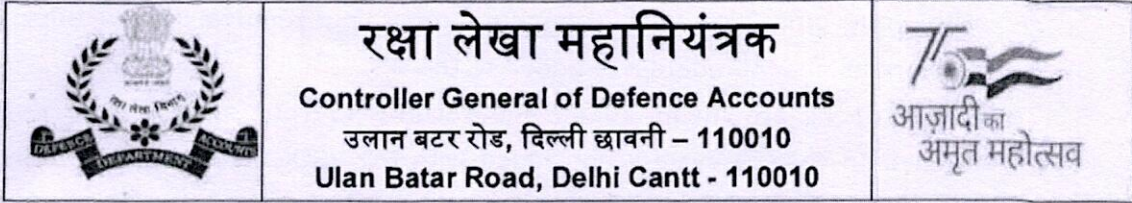
Topic wise list is enclosed below.

Sl.No.	Advisories
1.	Checklist for action taken report on NOC-SOC report.
2.	Does and Don'ts for WAN attached systems.
3.	How to install endpoint central (Patch) agents.
4.	Steps to disable the unused user accounts from your systems.
5.	Steps to disable multiple LAN Ips/ Ethernet Cards from system.
6.	Escalation Matrix for reporting DAD WAN connectivity issues.

All Officers In-charge are here-by directed to ensure that the advisories issued by HQrs. Office as mentioned above, are strictly followed by all the staffs under his supervision.

Enclosure: - As above.


(Kavya Tangirala)
DY. CISO



By Mail

No. IT&S/806/WAN Security/2024-25

Dated: 23/06/2025

To

All PCDA/CDAs
(As per List)

Sub: WAN Security- Action thereon

Reference: HQrs office letter no even dated 06.01.2025.

Please refer to the above mentioned reference where guidelines for security of DAD WAN network were shared with all Controller offices. In addition to the same reports generated by NOC-SOC solutions on various security parameters are shared with Controller offices frequently for necessary action at their end.

2. In this regard, it has been observed that the compliance report of many Controller offices is not being received at all or not being received on time. As such, the detailed guidelines for the action required are shared as attachment for your action please.
3. In this regard, a few points for further information are added herewith:
 - a) Please check the systems which are not added with NOC-SOC agents. The necessary action for installation of agents may be taken as per SOP attached herewith. In case of any issue help of NOC-SOC team may be taken.
 - b) After installation of agents in remaining systems, please share the list of non-pertaining systems with this HQ supported with proper remarks viz., not pertain to this organization, other device (printer, cctv camera, etc) in the list. This will be helpful to mark the same remarks and avoid further adding the device in your report.
 - c) Please note that systems removed from DAD WAN will be kept in database for 90 days by NOC-SOC agents. In case a system removed from WAN is still reflected in report, please mention the same in report and confirm that the same mac address/IP address does not add to network again.
 - d) It has been observed that offices are changing the IPs of system which is creating database of duplicate IPs in NOC-SOC. A list of such cases is shared

Checklist for action taken report on NOC-SOC report:

96

S. N.	Report	Description	Action required from Controllers end
i	Bandwidth utilization	Report is shared to inform about the WAN link availability for your organisation (MO and Sub Offices).	The bandwidth utilization provides the utilisation status of DAD WAN network in your office. In case of any issue regarding speed, the same may be shared with this office for upgradation as per requirement justification with report.
II	No of PCs without NOC SOC agents	Shows no of PCs in which the NOC SOC agent have not been installed.	Please ensure the Agent installation process for the given systems as per SOP attached an Annexure 1. The remaining IPs not having physical appearance, not added to WAN systems, peripheral devices like printers, servers and Other IP devices may be informed to this wing for necessary action and removal from your report. In case, a system added with NOC-SOC agent is mentioned as not installed the same may be updated for the agent as per SOP.
III	Computer Inventory	The report shows the hardware and OS details of the computers	It can be seen that Main office and sub office are still using very old PCs and their windows operating system (OS) are not supported by the Microsoft. The non-updation of OS renders the computer vulnerable to cyber-attacks. It is therefore advised to replace the older systems with new ones. Please ensure that latest version of OS is installed on your system.
IV	Downtime report	The WAN downtime status of the office for Monday to Friday from 9.00 to 18.00 Hrs	The bandwidth utilization provides the availability status of DAD WAN network in your office. In this regard, it should be ensured that routers are kept on during office hours as the same are being monitored by NOC-SOC and payments to ISPs are released accordingly. In case of technical issue the same may be shared as per attached escalation

			Microsoft. Therefore, PCs with Windows 7 & 8 are to be replaced with PCs with latest OS. The patch updation of the latest PC is to be done by NOC-SOC team. The plan for the same will be shared soon.
VIII	System Password	This report shows the status of passwords for the user accounts in WAN added systems	A number of users of offices are not using the password for accessing the computer. This also makes computer vulnerable to attack. The MODNET policy mandates multilevel (BIOS/OS/application) password for the computers. Please check the users of mentioned systems for adding password security without fail. The same may be confirmed with Hrs office for updation. The unused user accounts in the control panel may be disabled to avoid repetition of same in user name password report. The same may be done as per SOP in Annexure 2.
IX	Threat Events	This shows the threat events detected in the computers by the endpoint protection i.e. Antivirus	The antivirus deletes or blocks the suspicious activity based upon the policies enforced. The "would block" threat/ activity are those which are not covered in delete or block policy. This only reflects the possible threats detected by system. However, If an IP (system) shows maximum number of threats in the threats report, the said system may be isolated from network with information to NOC-SOC for further analysis of the possible threat. No further action is required at your end for the same.
X	Licenses	This shows the status of windows licenses installed in WAN added systems	Please check the systems for activated windows licenses. In case, the same is already activated please intimate NOC-SOC. Please ensure that pirated windows are not utilised in the systems for better security.
XI	No of PCs with Antivirus	Number of threats that needs to be	No further action is required at your end for the same.

Frequently Asked Questions

SNo	Query	Answer
1	How to transfer the data between two WAN connected computers	For transferring the data among the WAN connected PCs can be through NIC Email or through whitelisted USB drives. Main office can have 5 and sub offices can have 2 whitelisted USB drives. These drives are to be kept in the safe custody of nominated person(s). The data should not be retained on the drives after transfer and it should be deleted. It is to be noted that the whitelisted drives are not to be used on internet connected computers.
2	How to transfer the data from internet connected computer to a WAN computer and vice-versa	The same can be done through the briefcase utility of NIC email id as NIC email is available on DAD WAN as well. The briefcase can hold upto 1 GB of data. It may be ensured that once the data has been copied on the destined computer, the same is deleted from briefcase as well as its trash.
3	How to install a software on a WAN connected computer as USB, DVD/CD ROM are disabled.	A repository of software (http://10.51.174.198/) has been made in this office which is available on WAN. General purpose software like open office, adobe reader, browser etc are available on the server. In case, an office requires specific software, a formal request may be sent to this office for necessary action in the matter.
4	If important data are required to be copied from WAN connected computer to hard drive for backup, archival purpose.	The external drive can be whitelisted by the NOC SOC team. A formal letter for the same duly approved by the PCDA/CDA is to be forwarded to this office for the purpose. The details of officer responsible for custody of the external drive should be mentioned in the letter. It may be ensured that no data is kept on the drive after transfer.
5	What is the process,	The matter may be taken up with HQrs WAN team

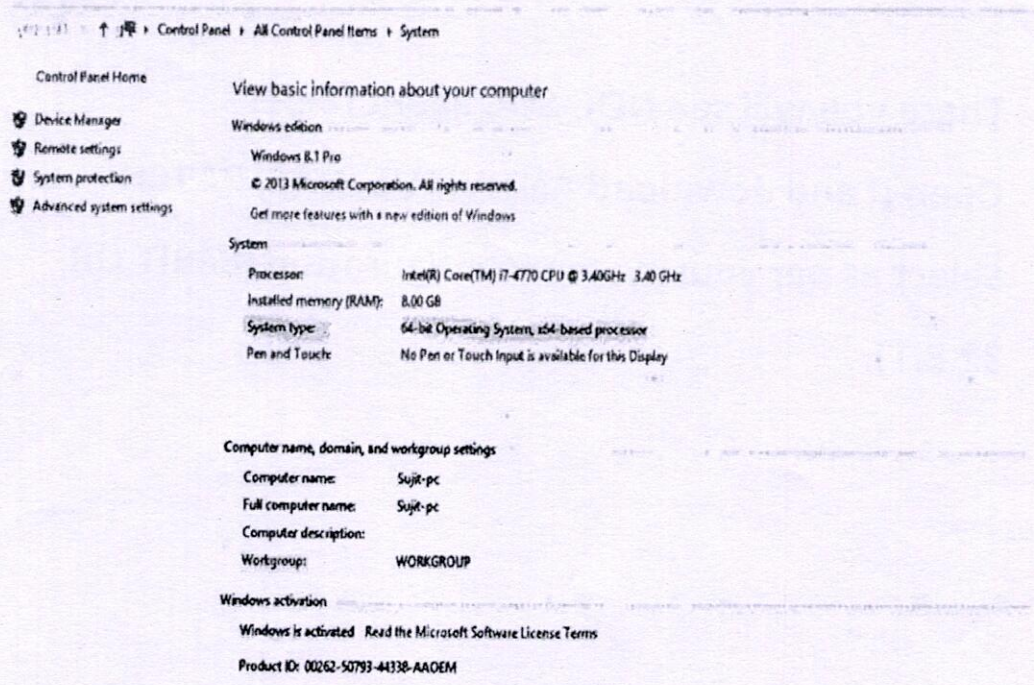
Does and Don'ts for WAN attached Systems:

- I. In no case, a PC should be connected to both internet and WAN.
- II. It should be ensured that as and when a new PC is to be connected to DAD WAN, its Operating system (OS) should be updated first and then it is should be connected to WAN. After that the NOC SOC software (Manage Engine Endpoint Central and Trellix antivirus) should be installed in consultation with NOC-SOC team at HQrs office.
- III. Personal laptops should not be connected to DAD WAN.
- IV. The office staff may be sensitized about the basic cyber security practices circulated by this office time to time and precautions to be taken while using WAN and internet. Some of the recommended practices are attached.
- V. Use of internet for carrying out official work may please be minimized.
- VI. An internet connected PC should not be straight away connected to WAN. It should be formatted and after afresh Installation & updation of OS, it is to be connected to WAN. Backup of data should be taken before formatting.
- VII. The users of the computers may not be given the administrative privileges. The administrative rights of a computer should be with the IT team of the office. The users may be given the standard user rights only.
- VIII. It has been observed that sometimes the IP address assigned to a WAN PC is changed, this creates reconciliation issues in the reports generated by the NOC SOC team. Therefore, it is advised that the change of IP address of a WAN PC may be avoided. If a PC is to be formatted due to OS crash or technical reason etc, it should be given the same IP address as assigned earlier. A register may be maintained by the maintenance team for the purpose. Also, giving standard rights on the PC to a user will avoid the issue of change of the address by the user himself.

HOW TO INSTALL ENDPOINT CENTRAL (PATCH) AGENTS

Step – 1 Check System Configuration

- Right click on THIS PC.
- Go to PROPERTIES.
- There you will see system type it can be 32bit or 64bit.



Step – 2 Install the Software's.

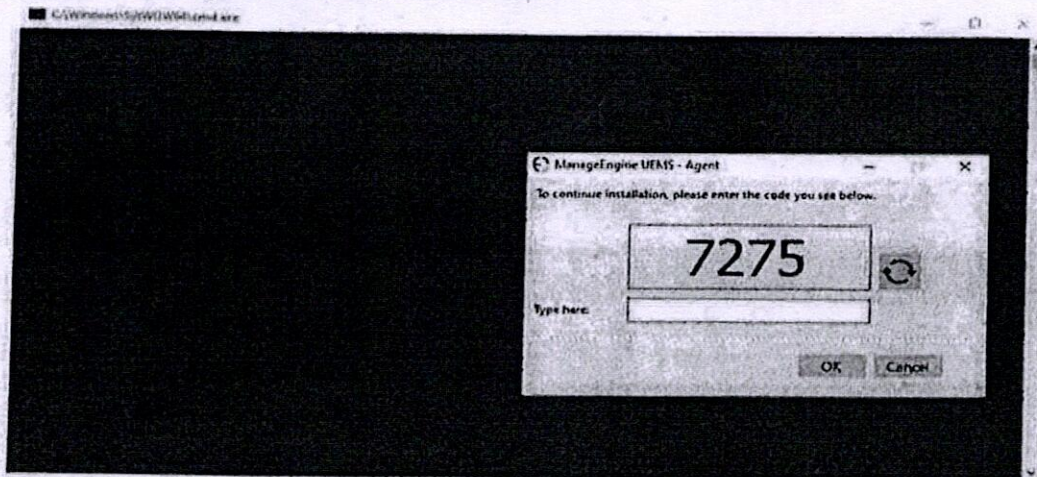
- Go to downloads
- There you will see Software.

Name	Date modified	Type	Size
ENS-FramePkg	02-01-2025 09:58	Application	18,123 KB
SC - C:\OubC\Tpm6B46+vaZUs65oMdJAKi+ib3scd1zLEQhz2DhdUPIQEAHs9TT	02-01-2025 09:58	Application	2,727 KB
UEMS AGENT (2)	02-01-2025 09:58	Application	36,099 KB

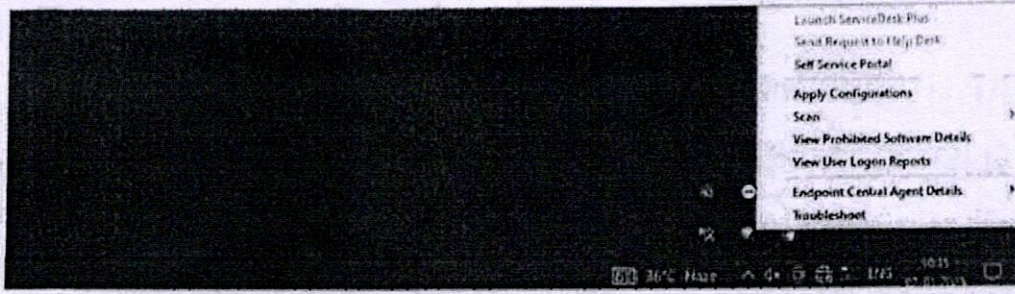
Start with UEMS agent run it as administrator.

Name	Date modified	Type	Size
ENS-FramePkg	02-01-2025 09:58	Application	18,123 KB
SC - C:\OubC\Tpm6B46+vaZUs65oMdJAKi+ib3scd1zLEQhz2DhdUPIQEAHs9TT	02-01-2025 09:58	Application	2,727 KB
UEMS AGENT	02-01-2025 09:58	Application	36,099 KB
UEMS AGENT	01-01-2025 10:36	Application	36,099 KB
WAN_LINKS	01-01-2025 09:47	Microsoft Excel W...	
BSNL-DAD-C	31-12-2024 10:31	Microsoft Edge P...	1,2
BSNL-DAD-C	31-12-2024 10:30	Microsoft Edge P...	1,2
UTILIZATION	31-12-2024 10:22	Microsoft Excel W...	
WAN_LINKS	31-12-2024 09:55	Microsoft Excel W...	

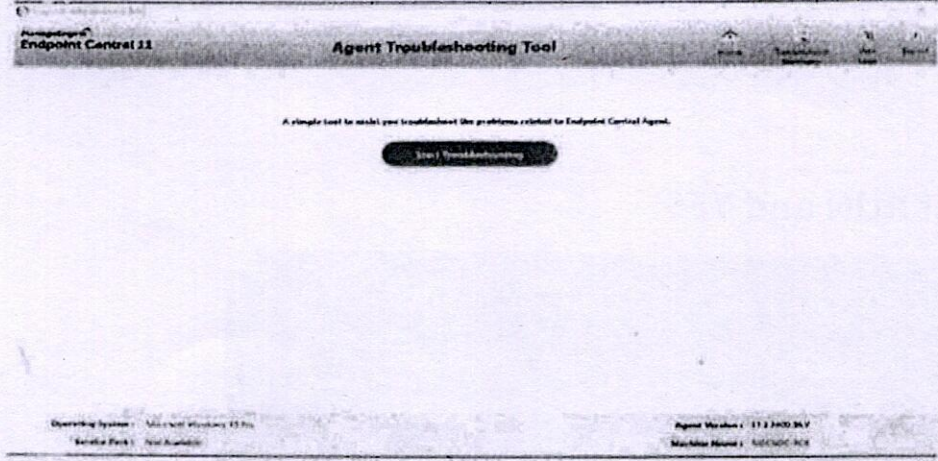
➤ Fill the Captcha and click ok.



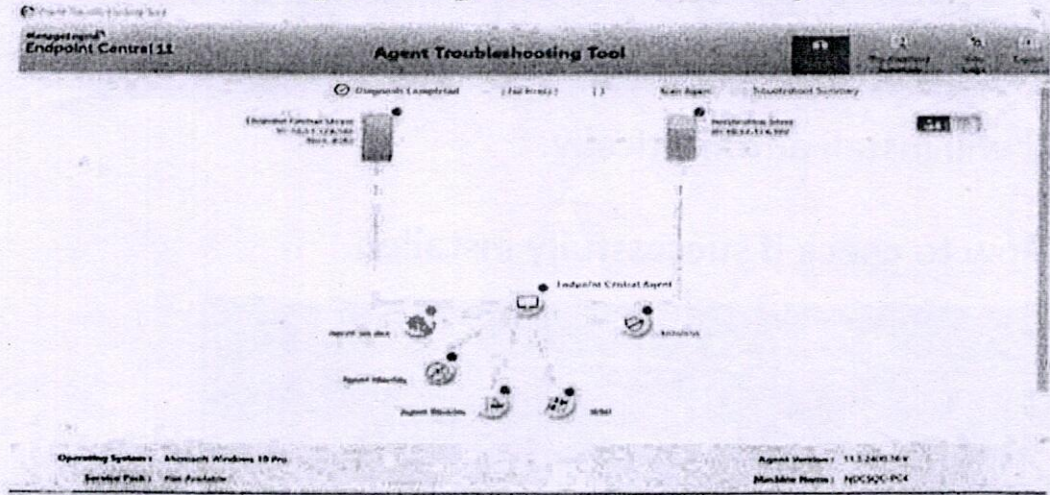
➤ Right click on it and select troubleshoot



➤ Click on start troubleshooting



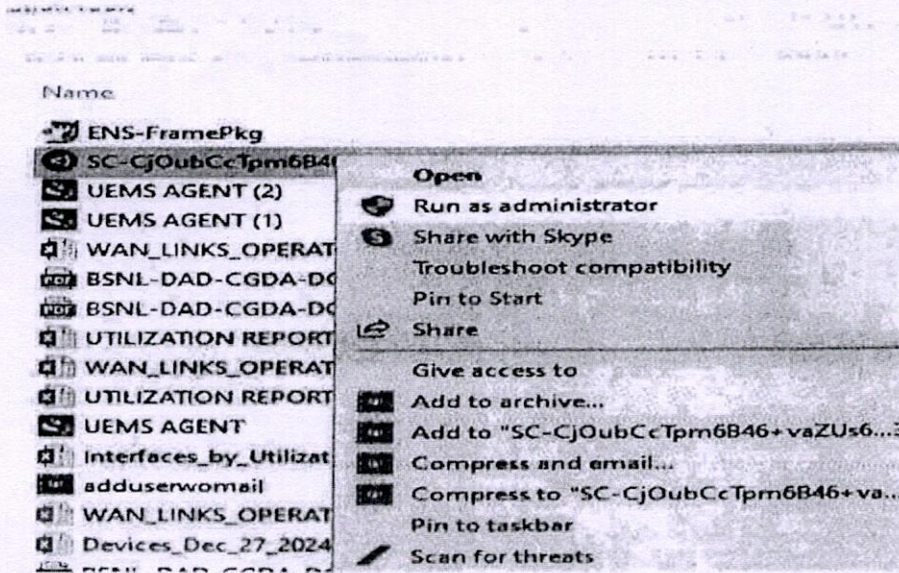
➤ If all status are green agent is successfully installed



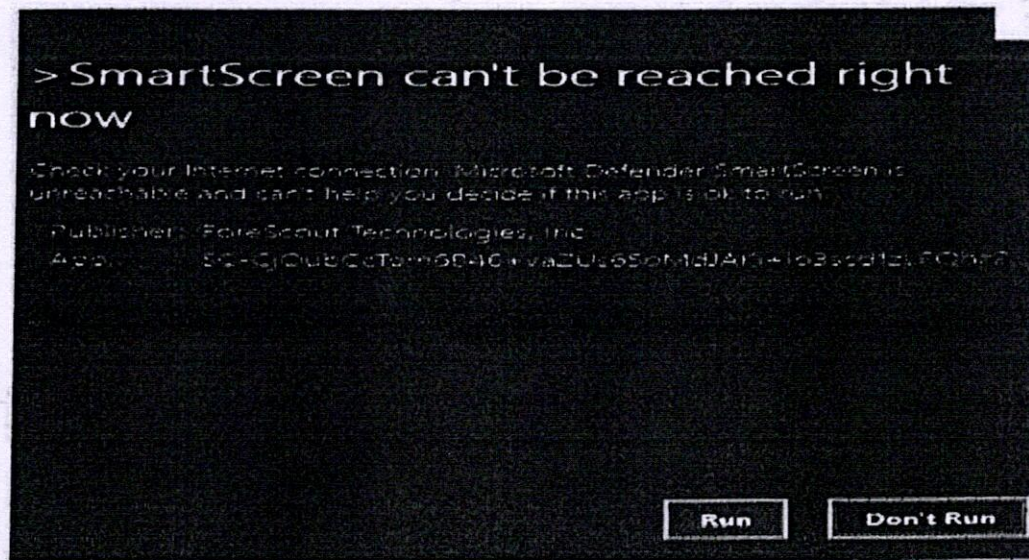
Finish

ForeScout installation

- Run SC-CjOubCcTpm6B46+vaZUs65oMdJAKi+ib3scd1zLEQh z2DhdUPfQEAAHe5gTT as administrator.



- Click on Yes and Run



- It will install automatically.

STEPS to disable the unused USER accounts from your systems

The steps for the same are as follows: -

- Go to **Control Panel** → **Network and Sharing Center**
 - Click **Change adapter settings** on the left
 - Right-click on the network adapter (Ethernet, Wi-Fi, or Virtual) → select **Properties**
 - Select **Internet Protocol Version 4 (TCP/IPv4)** → click **Properties**
 - Click **Advanced...** button
 - In **Advanced TCP/IP Settings**, under the **IP addresses** section:
 - You will see all configured IPs.
 - Select the extra IP addresses one by one and click **Remove**
 - Click **OK** → **OK** → **Close** to save settings
- Disable for **IPv6**.

Step's to disable multiple LAN IPs/ Ethernet Cards from system

The steps for the same are as follows:-

Right-click on This PC (or "My Computer") → click **Manage**

➤ OR press Win + X → select **Computer switches Management**

➤ In the left pane, expand:

System Tools → **Local Users and Groups** → click on **Users**

➤ In the middle pane, you will see a list of user accounts.

➤ **Right-click on the user** you want to disable → click **Properties**

➤ In the **General tab**, check the box:

Account is disabled

➤ Click **Apply** → **OK**

➤ Close Computer Management.

The user is now disabled and will not be able to log in.

71

1st Escalation Level - Service Desk (Immediate)

S. No.	Name of Service Desk Personnel	Area Cover	Phone/Mobile	Email	Customers Handled
1	Help Desk all India (24*7 Support)	PAN INDIA	022-68331676 022-68331675 022-68331674 9136941136/7738435123 (Note :- 02269158826/ 02269156827/ 02269158828	mplshelpdesk@ebixcash.com machhindra.bhunia@ebixcash.com ajul.nagpure@ebixcash.com	ALL CLIENTS (DOKE BOOKING)

2nd Escalation Level - Service Desk (0H to 4H)

S. No.	Regional Helpdesk Team	Area Cover	Phone/Mobile	Email	Customers Handled
1	North 2 Regional Helpdesk	Uttar Pradesh	Jeeva-7398764332	bharsupport@ebixcash.com ajaykumar.tiwari@ebixcash.com	Customers Handled All Clients
2		Bihar/Jharkhand	Amlesh Murti-9334251263	amlesh.murti@ebixcash.com	All Clients
3	East Regional Helpdesk	West Baengal / Assam/Orissa/North East	Helpdesk East - 033-4600 4205/4203/4211/4209 Helpdesk TL - Binod Shaw - 9831396755, Shubhankar TL- 9749883177, 8290342538	support.east@ebixcash.com / binod.shaw@ebixcash.com	All Clients
4	West Regional Helpdesk	Maharashtra/Goa/Pune	Chanchal 8888007348 Gauri 7773924203	support.west@ebixcash.com	All Clients
5		Madhya Pradesh	Manoj Chourasia - 9827566386	Sunnykumarsahoo7509@gmail.com	All Clients
6		Chhattisgarh	Yogendra-9131094080	YogendraIwar0801@gmail.com	All Clients
7		Mumbai	Kirti- 7066434720 PM Pankaj Mhatre - 9833401443	pankaj.mhatre@ebixcash.com umesh.rakhasiya@ebixcash.com	All Clients
8	Gujarat Regional Helpdesk	Gujarat	Bhavik-9726206662	bhavik.shekhar@ebixcash.com	All Clients
9	North1 Regional Helpdesk	Uttarakhand/Delhi/Punjab/Haryana/Jammu Kashmir	Tamna-7906292428/Neha-8860866779	support.north@ebixcash.com dneha2783@gmail.com tamamna252627@gmail.com	All Clients
10	South Regional Helpdesk	Karnataka	Rakshil- 9741472865 Thamilzh- 8667089640 080-66561013/14	cockk@ebixcash.com	All Clients
11		Kerala	DV Jain-9020805300	dvjain@ebixcash.com	All Clients
12		Tamil Nadu	NAGRAJ- 9080379567 Jahangheer-9626739327 9962095158	chennaisd@ebixcash.com /chennaihelpdesk@ebixcash.com	All Clients
13		Andhra Pradesh/Telangana	Ranjita-9666795999	trinahyderabad@gmail.com /	All Clients
14		Team leader Uttarakhand	Monu-09410786186	monu.rajpud2051@gmail.com	All Clients
15		Kolkata Team leader	Sudipta Roy Chowdhury- 09836930066 Subhankar Singha - 09749883177	sudipta.roychowdhury@ebixcash.com subhankar.singha@ebixcash.com	All Clients

3rd Escalation Level - Regional Service Managers (Project Manager)(4H to 8H)

S.No.	Name of Service Manager	Area Cover	Phone/Mobile	Email	Customers Handled
1	Amlesh Murti	JHARKHAND	9334251263	amlesh.murti@ebixcash.com	All Clients

22

Sr.No.	Name of Service Manager	Area of coverage (Name of Zone)	Phone/Mobile	Email	Area of coverage (Name of states)
1	Amar Jha	PAN INDIA	9892287282	amar.jha@ebxcash.com	All Clients

Railtel Escalation (Western Region)

(25)

Serial No.	Who will escalate	When to escalate	Designation of person to be escalated	Name Phone/Mobile no	Email Id
1	Customer /NOC	Immediately	Railtel CNOC - Delhi (DOCKET Booking)	1800117245 (Central Noc)	mplshelpdesk@railtelindia.com mpls_wr@railtelindia.com
2	Customer/ NOC	After 1 hrs	Regional NOC -Mumbai	Mob.No:7710039394 ,8828407538 +91 1242714000 : 6141	mpls_wr@railtelindia.com, mplsnoc@railtelindia.com
3	Customer /NOC	After 2 hrs	S. Manager NOC	Shift Incharge 9004444161 9004444122 +91 1242714000 : 6215,6218	santosh.sinha@railtelindia.com, amrut@railtelindia.com
4	Technical manager	After 3 hrs	S. Manager NOC	Mr. Amit Kumar (9004444164) +91 1242714000 : 6212	amit_kumar@railtelindia.com
5	Technical manager	After 4 hrs	AGM O&M	Mr. Anoop manocha Mobile No.91790 83400	manocha_anoop@railtelindia.com
6	Atleast SM level (Customer Organisation)	After 5 hrs	DGM Field	Mr. Girish Kakre Mobile No.9900444449 (For Mumbai /KRCI/Goa Section) Mr. Suresh Mahabha Mobile No.9090444145 (For Pune-MRG-3D-SUR Section) Mr. Anoop manocha MobileNo.91790 83400 (ForBFL, Kota, Jabalpur,Katlam,IndoreSection Mr. Mukesh Barhore Mobile No. 9974151503 (For Ahmedabad, Gandhidham, Bhavnagar, Junagadh Section) Mr. Santosh Dubey Mobile No:- 9179044016 (For Bhusawal,Nagpur section)	girishkake@railtelindia.com s. mahobya@railtelindia.com manocha_anoop@railtelindia.com mukesh@railtelindia.com santosh. dubey@railtelindia.com
7	Atleast DGM level (Customer Organisation)	After 6 hrs	JGM NOC	Mr. Rajendra Malakar 9004444133	rajendra.malakar@railtelindia.com

Railtel (South Region)

DETAILS	Docket booking	AFTER 1HR	AFTER 2HRS	AFTER 4HRS	AFTER 6HRS	AFTER 8 HRS
NAME	Toll-free: 1800117245 EXT. 11 Ph no.-011-22900400 EXT 11	L1 Support 9704333690 .07032714112	Mr. Ramu (7349249761)	Mr. U.P. Raju-9849019407	Shri A Siva Prasad (9849658107)	Shri. Shalendra Singh (9392901010)
DESIGNATION	24x7 MPLS Helpdesk	L1 support	Sr. Manager/MPLS	Asst. GM/MPLS	DGM/NOC	GM/TW/SC
EMAIL ID	mpls@railtelindia.com	l1support@railtelindia.com mpls_sr@railtelindia.com	ramu@railtelindia.com	up.raju@railtelindia.com	asprasad@railtelindia.com	shalendra.singh@railtelindia.com

75

20

Railtel (East Region)

Escalation Matrix of MPLS NOC ER					
S.N.	Designation of person to whom it is to be escalated	When to escalate	Who will escalate	Name Phone/Mobile no	Email id
1	MPLS CNOC Helpdesk	Immediately	Customer NOC	P&T: 011-22900400 Toll Free No. 1800117245	to.mpls@railtelindia.com cc.mpls_erp@railtelindia.com, cc.mpls@railtelindia.com
2	MPLS NOC Eastern Region	After 30 Minutes	Customer NOC	Mobile No:9007044145 Alternative Tollfree : 1800117245 say Extn 8410 to operator ,9007044148 (SBI dedicated)	mpls_erp@railtelindia.com
3	Deputy Manager/ MPLS ER NOC	After 1 hrs	Customer NOC	Sh. Selu Verma 07044820178	seluverma@railtelindia.com
4	Senior Manager/ MPLS ER NOC	After 3 hrs	Customer NOC	Sh. Siddharth Kumar 09007044134	siddharth.km2003@railtelindia.com
5	AGM/NOC	After 5 hrs	Atleast AGM level (Customer Organisation)	Sh. Anand Swarop srivastava 7044820154	anandsrivastava@railtelindia.com
6	GM/OP	After 6 hrs	Atleast DGM level (Customer Organisation)	Sh. Arun Michael Mob No:- 9007044200	arun.michael@railtelindia.com