



SystemMatch Monitor End User Guide

Customer instructions for setting up sites devices checks alerts and reports

For customer administrators and operators. This guide does not include server deployment or database administration.

Version date 19 September 2026

This guide starts after SystemMatch has created your trial or paid account. A customer administrator can complete the setup from the web console and one Windows or Linux machine at each site. Install only one SystemMatch agent on each physical computer or virtual machine. The agent only makes outbound encrypted connections to SystemMatch and opens no inbound port.

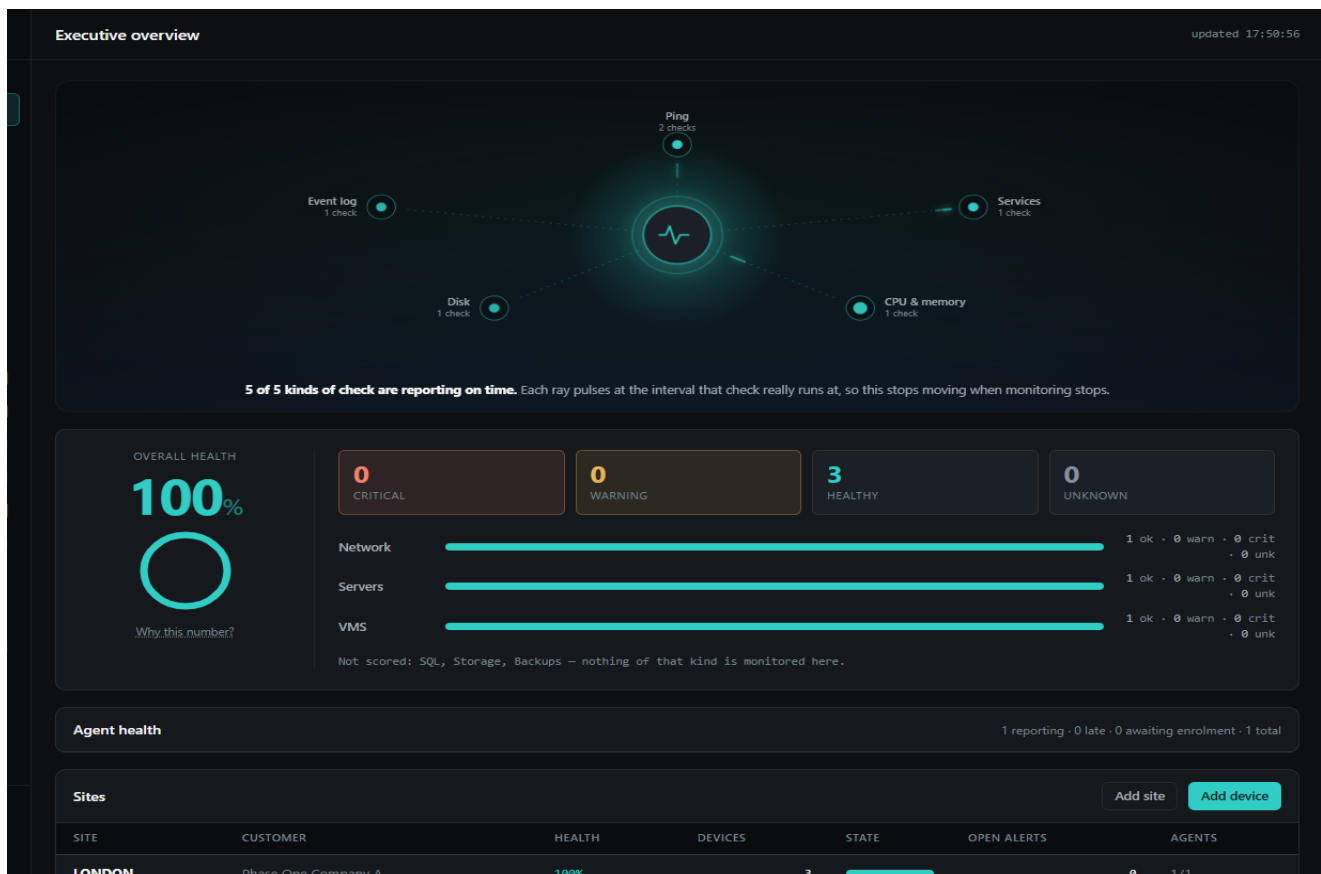
You need	Where to get it
Your SystemMatch account setup	The secure one time link in the welcome email from SystemMatch
One agent machine per site	A Windows or Linux machine that stays on and can reach the devices
Administrator access on the agent machine	Your own IT administrator or system integrator
Device names and addresses	Your device list network plan or DHCP reservations

Keep the one time enrolment token private. The installer uses it once and it cannot be recovered later. If it is lost or Reissue token is clicked again, use only the newest token shown by the console.

First sign in

1. Open the welcome email sent by SystemMatch and check that it names your company.
2. Choose the secure account setup link. It works once and expires after 60 minutes.
3. Create your own password. SystemMatch never sends a temporary password by email.
4. Sign in at <https://monitor.systemmatch.co.uk/monitor/>.
5. Enable multifactor authentication if your organisation requires it, then confirm the company name before adding sites or users.

For security the platform creates an internal random bootstrap credential that is never displayed or emailed. The password you choose through the setup link replaces it. If the link expires use I have forgotten my password on the sign in page to request a new one.



The executive overview is the starting page after sign in

The coloured state has a precise meaning

State	Meaning	Action
OK	The latest result is within its configured limits	No action
WARNING	A limit has been crossed or a result is degraded	Investigate during the agreed support window
CRITICAL	The device or monitored function has failed	Respond using your escalation process
UNKNOWN	The agent could not prove the state	Read the message and correct the assignment permissions or platform mismatch
LATE	The expected result has not arrived	Check the agent service internet connection and machine power

Create a site

A site is a physical location or a network boundary. Create one before registering its agent.

6. Select Sites and choose Add site.
7. Enter the site name address reference and time zone.
8. Choose Create site.
9. Open the new site and check that it shows zero devices and no agent yet.

The screenshot shows the 'Add a site' dialog box in the SystemMatch Monitor interface. The dialog is titled 'Add a site' and has a close button (X) in the top right corner. It contains the following fields and options:

- Customer:** A dropdown menu with 'Phase One Company A' selected.
- Site name:** A text input field with 'London' entered. Below it, a note says 'How this location is known — usually the town or the building.'
- Reference:** A text input field with 'Your own job or site reference (optional)' entered.
- Address:** A text input field with 'Optional' entered.
- Time zone:** A dropdown menu with 'Europe/London' selected. Below it, a note says 'Used for maintenance windows and report scheduling.'

At the bottom of the dialog are two buttons: 'Cancel' and 'Create site'.

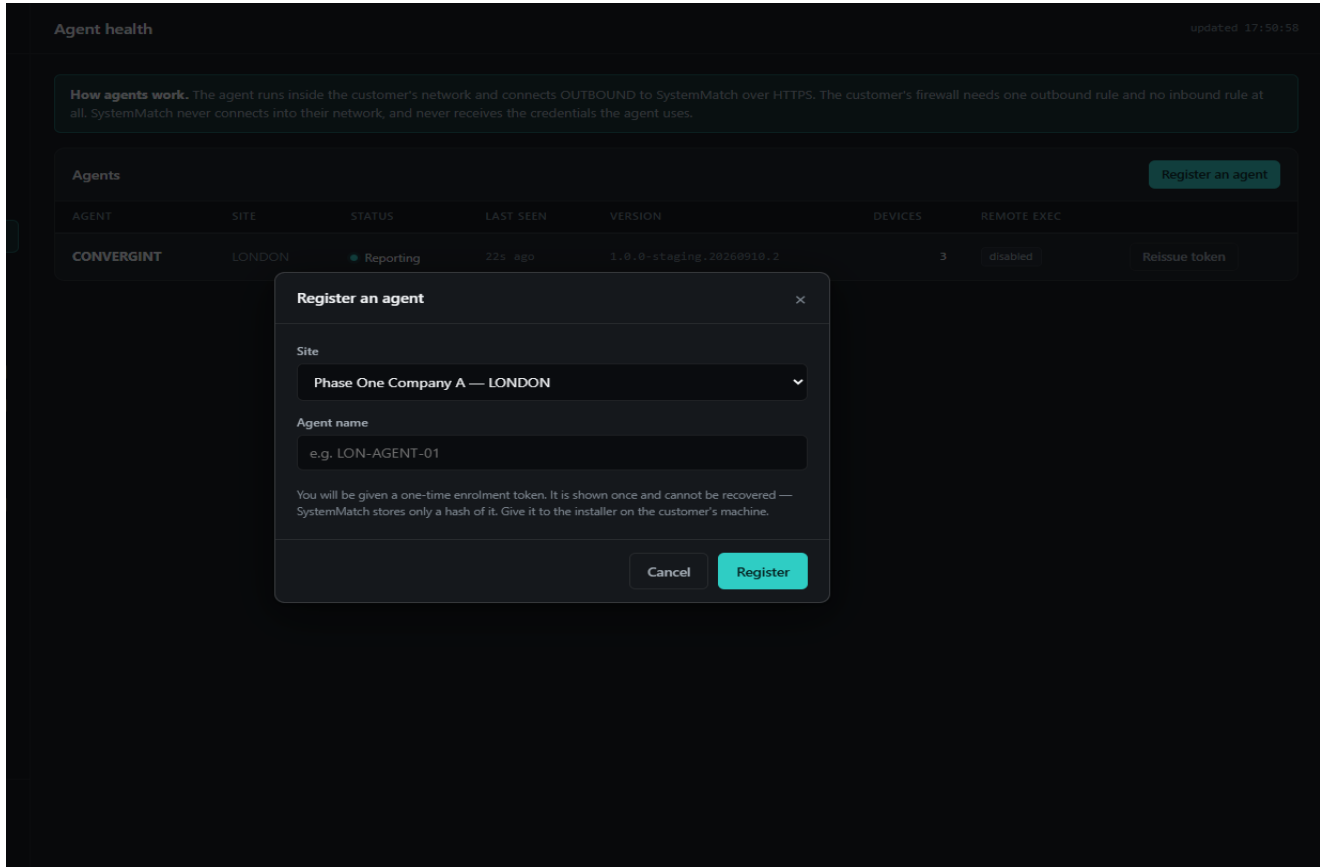
The background of the screenshot shows the 'Sites' page. It has a top bar with 'Sites' and 'updated: 17:59:57'. Below the top bar is a 'Ping' status indicator showing '2 checks' with a green dot. The main content area shows a '3' in a green circle, indicating '3 HEALTHY' sites, and a '0' in a grey circle, indicating '0 UNKNOWN' sites. Below this are three horizontal bars representing different health metrics, each with a status of '1 ok · 0 warn · 0 crit · 0 unk'. At the bottom, there is a table with columns: SITE, CUSTOMER, HEALTH, DEVICES, STATE, OPEN ALERTS, and AGENTS. The first row shows 'LONDON' under SITE, 'Phase One Company A' under CUSTOMER, '100%' under HEALTH, '0' under DEVICES, '1' under STATE, '0' under OPEN ALERTS, and '1' under AGENTS.

Add a site using the customer name and local time zone

Use one agent for each site and one installed agent per physical computer or virtual machine. The agent must be able to reach the private device addresses at that site. A cloud server cannot directly ping a camera on a private address such as 192.168.1.20. If two sites need separate agents, provide two always-on machines or virtual machines.

Register and install a Windows agent

10. Open Agent health and choose Register agent.
11. Select the site, give the agent a clear name and choose Register.
12. Choose Copy Windows install command. Do not copy or edit the token separately.
13. Download the Windows 64 bit ZIP and choose Extract all in File Explorer.
14. Open Windows PowerShell as administrator and change to the extracted folder.
15. Paste the complete command copied from SystemMatch and press Enter.



Register the agent for the correct site. After registration use Copy Windows install command

```
Set-ExecutionPolicy -Scope Process Bypass -Force
# Paste the complete command copied from Agent health.
# The real command already contains the correct server token and agent name.
```

One agent per computer

A Windows service uses one protected identity store in C:\ProgramData\SystemMatch\Agent. Installing another site agent on the same computer would replace that identity. The installer now stops before making changes when it finds an existing agent. Run each additional site agent on a different always-on computer or virtual machine.

Confirm the service

```
Get-Service SystemMatchAgent
& "C:\Program Files\SystemMatch\Agent\systemmatch-agent.exe" status
```

The service status should be Running. Return to Agent health and wait for Reporting with a recent Last seen time. If enrolment succeeded but service installation failed, do not enrol again until you have checked whether the service exists.

Repair an existing Windows agent

Use this path only for the same agent row and the same computer. In Agent health choose Reissue token, then choose Copy existing-agent command. Open PowerShell as administrator, paste the complete command and wait for the service to return to Reporting. Clicking Reissue token again invalidates the command already copied.

Register and install a Linux agent

16. Register the agent in the console and copy the one time token.
17. Download the Linux 64 bit archive and extract it on the customer machine.
18. Open a terminal in the extracted folder.
19. Run the installer below with your token and agent name.

```
chmod +x install-agent.sh
sudo ./install-agent.sh \
  --server https://monitor.systemmatch.co.uk \
  --token "PASTE-THE-ONE-TIME-TOKEN" \
  --name "LONDON SITE AGENT"
```

Confirm the service

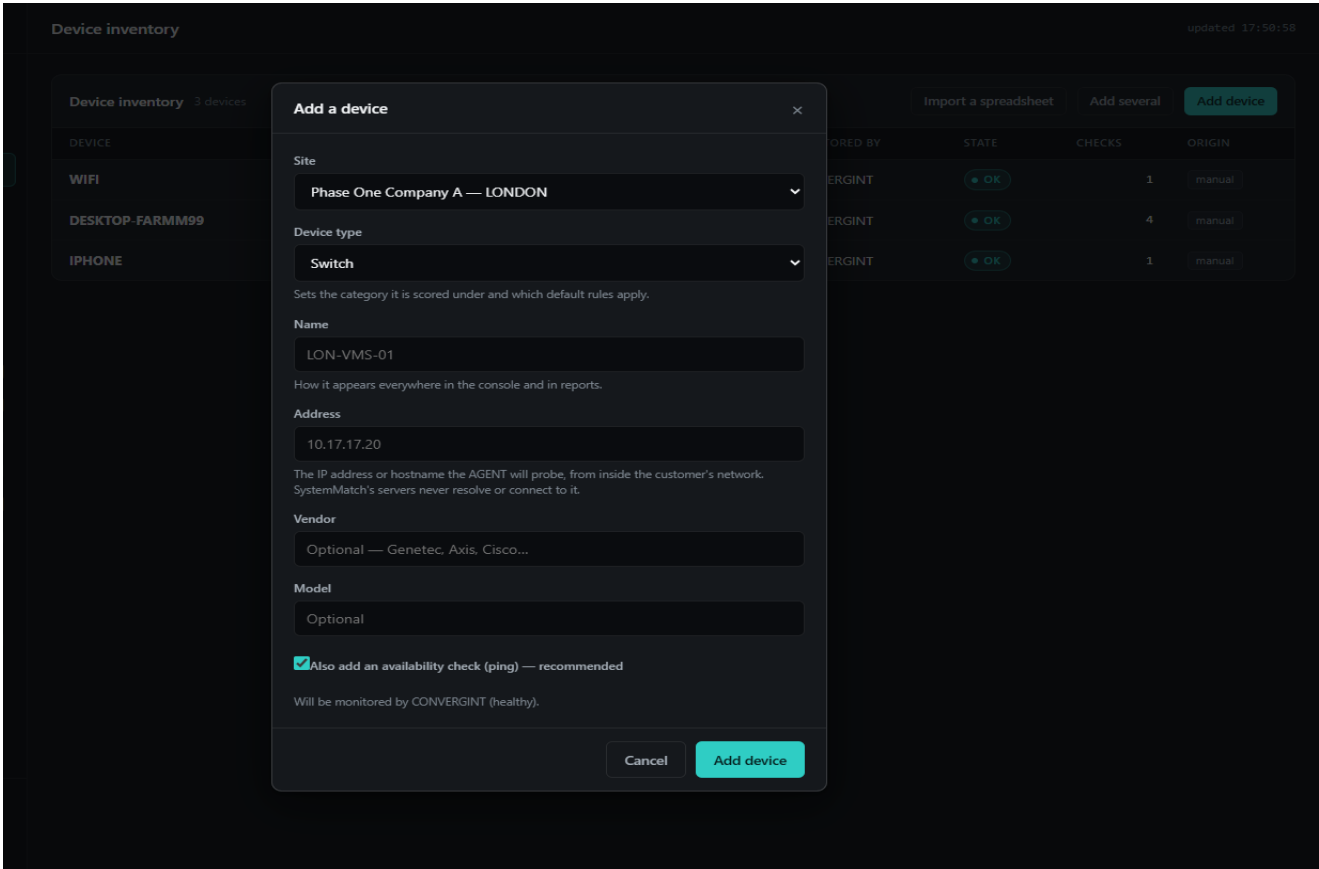
```
sudo systemctl status systemmatch-agent --no-pager
```

The agent needs outbound HTTPS on TCP port 443 to monitor.systemmatch.co.uk and working DNS resolution. It does not need an inbound firewall rule. On Fortinet or another managed firewall allow only the dedicated agent machine to make that outbound connection. The monitored cameras servers switches and other devices do not need internet access. If the entire site has no internet path SystemMatch cannot receive live results and the agent will show Late then Offline. If the site uses an authenticated web proxy ask SystemMatch support whether the current agent build supports that proxy before installation.

Add devices

A device is anything you want the site agent to test. Use a stable address. Reserve the address in DHCP or use a static address so a different device is not later given the same IP.

- 20. Select Device inventory and choose Add device.
- 21. Select the site and the agent that can reach the device.
- 22. Enter a clear name device type and IP address or host name.
- 23. Leave Create an availability check selected if you want an immediate ping test.
- 24. Save and wait for the first result.



Add a device and assign the agent at the same site

Device type	Recommended first checks
Camera encoder or intercom	Ping then TCP for the management or media port when known
Router switch firewall or UPS	Ping TCP or HTTP now. Interface and environmental SNMP monitoring is on the roadmap
Windows server or VMS server	Ping Windows service disk space CPU and memory and Windows event log
Linux server	Ping disk space CPU and memory and Linux software RAID where applicable
SQL Server host	Ping TCP 1433 Windows service disk CPU and event log. Database query monitoring is on the roadmap

Add network checks

Open the device and choose Add check. Only checks in Available now or Available with a stated platform limit can be selected.

Check	Use it for	Important settings
Ping	Basic reachability	Four probes is a sensible start. Packet loss can produce a warning even when the device answers
TCP port	A service listening on a known port	Enter the port such as 443 554 1433 or a vendor port
Web interface	An HTTP or HTTPS page	Expected status and optional text. Allow an invalid certificate only for a known self signed device

A successful ping proves only that the address answered. Add a port or web check when the device can answer ping while its application is stopped.

Monitor Windows services

Windows service monitoring is live and reads the machine where the Windows agent is installed. It does not control the service and cannot start or stop it.

25. Install the SystemMatch agent on the Windows machine that owns the service.
26. In PowerShell run the command below to find the service short name.
27. Open the matching device choose Add check and select Windows service.
28. Enter one or more short service names separated by commas.
29. Use W32Time to test Windows Time. Stop it briefly then confirm CRITICAL and start it again to confirm recovery.

```
Get-Service | Select-Object Name, DisplayName  
Get-Service W32Time
```

Example service name

```
W32Time
```

Use the Name column, not the friendly DisplayName. A check on a different computer cannot read the service and should report UNKNOWN rather than OK.

Monitor disk space and host resources

These checks measure the computer where the agent runs. Attach them to the device record representing that computer.

Disk space

30. Choose Add check and select Disk space.
31. Enter volumes such as C:\ or D:\ separated by commas. Leave blank to watch the installation volume.
32. Start with 85 percent warning and 95 percent critical.
33. For a large recording array also set Critical below GB free. Either limit can raise the alert.

The screenshot shows the 'Add a check to WIFI' dialog box in the SystemMatch Monitor interface. The dialog is for configuring a 'Disk space' check. The 'Check type' is set to 'Disk space'. The 'Name' is 'Disk space'. The 'Volumes' are 'C:\, D:\'. The 'Warning at (% full)' is '85'. The 'Critical at (% full)' is '95'. The 'Critical below (GB free)' is 'optional'. The 'Interval (seconds)' is '60'. The 'Failures before alerting' is not visible. The background shows the 'Device' page with a 'WIFI' check status of 'OK' and a table of checks.

CHECK	TYPE
Availability	ICM

Configure the volumes and warning and critical limits for disk space

CPU and memory

34. Choose CPU and memory.
35. Start with 80 percent warning 90 percent critical and five minutes sustained.
36. Set a minimum available memory value only when the application vendor specifies one.

Disk and CPU thresholds can be adjusted later. Do not set the warning and critical values to the same number because the warning state would have no useful range.

Monitor Windows Event Viewer

Windows event log monitoring is live on Windows agents. The agent filters locally and sends only counts provider names and event IDs. It never sends the message text because messages can contain user names paths IP addresses and SQL text.

- 37. Open the Windows server device and choose Add check.
- 38. Select Windows event log.
- 39. Choose System Application or Security and select the levels to count.
- 40. Optionally enter a provider and event IDs to reduce noise.
- 41. Choose the look back window and warning and critical counts.

Purpose	Log	Provider	Event IDs
Disk errors	System	Disk	7 11 51 52
Unexpected reboot	System	EventLog	6008
Service crash loop	System	Service Control Manager	7031 7034
SQL data integrity warning	Application	MSSQLSERVER	823 824 825
Failed logons	Security	Any	4625

Configure alerts

42. Open Who gets told and choose Add people.
43. Name the recipient list and enter one or more email addresses.
44. Choose which severities the list should receive and turn the list on.
45. Choose Send a test and confirm delivery before relying on alerts.
46. Cause a safe test fault such as stopping Windows Time then confirm one alert and one recovery email.

SystemMatch sends on a state transition. It does not send a new message on every check while the same fault remains open. Repeated result counts in the console do not therefore mean repeated emails should arrive.

If a test email arrives but a fault email does not check that the alert is new the recipient list includes that severity and the alert was not already open before the list was created.

Use alerts and reports

Alerts

47. Open Alerts and filter by customer site state or time.
48. Open an alert to read the latest message and the recommended action.
49. Acknowledge it when somebody has taken ownership.
50. Resolve the underlying fault. Recovery is recorded when the next good result arrives.

Reports

51. Open Reports and choose the customer date and scope.
52. Generate a PDF for an immediate customer review.
53. Daily reports cover the previous local calendar day and are sent after midnight to enabled reporting recipients.
54. Check the report delivery status if an expected email does not arrive.

Add customer users

55. Open People and choose Invite person.
56. Enter the work email display name and role.
57. Give Administrator only to people who manage sites users agents and settings.
58. Give Operator to people who investigate and acknowledge alerts.
59. Give Viewer to read only customers and managers.
60. Choose Create invitation. SystemMatch emails the secure one time link automatically and also shows it once as a manual fallback.
61. The invited person creates their own password. No password is sent by email.
62. Review active sessions and remove access when a person leaves.

The screenshot displays the 'People' management page in SystemMatch Monitor. At the top, it says 'People' and 'updated 17:51:01'. Below this is a table of users:

NAME	EMAIL	ROLE	STATUS	LAST SIGNED IN	SESSIONS
Phase One Owner A	phase1.owner.a@example.test	Administrator	Active	5s ago	5
Phase One Viewer	phase1.viewer@example.test	Viewer	Active	never signed in	0

An 'Invite somebody' button is visible in the top right. Below the table, there is an 'Invitations' section with a table showing one invitation:

NAME	ROLE	STATE
Phase One Viewer	viewer	ACCEPTED

An 'Invite somebody' modal is open in the center, containing the following fields:

- Email address:** A text input field.
- This becomes their sign-in name.** A text input field.
- Their name:** A text input field.
- Role:** A dropdown menu with 'Viewer' selected.
- Read-only access to dashboards, devices, alerts and reports.** A checkbox.
- Create invitation:** A button.

Invite each person with the least access needed for their work

Roles and permissions

updated 17:52:13

Roles

ROLE	WHAT IT IS FOR	PERMISSIONS
Administrator	Full control of this company: sites, devices, agents, users, notifications and settings.	19
Operator	Day-to-day operations: acknowledge alerts, set maintenance, manage devices and checks. Cannot manage users or company settings.	13
Viewer	Read-only access to dashboards, devices, alerts and reports.	8

What each role can do

19 permissions

PERMISSION	KEY	ADMINISTRATOR	OPERATOR	VIEWER
AGENTS				
View agents See agent status and health.	agents.read	yes	yes	yes
Manage agents Register, reissue and revoke agents.	agents.write	yes	-	-
ALERTS				
Acknowledge alerts Acknowledge an alert and add a note.	alerts.acknowledge	yes	yes	-
View alerts See open and historical alerts.	alerts.read	yes	yes	yes
Manage maintenance Put devices and sites into maintenance mode.	maintenance.write	yes	yes	-
View notifications See notification recipients and rules.	notifications.read	yes	yes	yes
Manage notifications Change who is notified and when.	notifications.write	yes	-	-
COMPANY				
View company	company.read	yes	yes	yes

Review the permissions attached to each customer role

Role	Typical user	Use
Administrator	Customer IT lead or system integrator lead	Sites devices agents users and customer settings
Operator	Service desk or maintenance engineer	Monitor alerts investigate and acknowledge
Viewer	Customer manager or auditor	Read dashboards alerts and reports

Give a system integrator portfolio access

A system integrator does not connect directly to a customer's private network. The site agent sends monitoring results outbound over HTTPS to SystemMatch. The integrator signs in to the public SystemMatch console from its own office and sees only customers that have granted that account access.

63. Create one named SystemMatch account for each Convergent engineer or service desk user. Do not share one account.
64. From each customer open People and invite the same Convergent work email as Viewer Operator or Administrator according to the contract.
65. The engineer accepts the first invitation and creates a password. Later invitations add customers to the same account without changing that password.
66. After sign in choose All customers for the combined portfolio dashboard or select one customer for its sites devices agents alerts and reports.
67. Use Viewer for oversight Operator for investigation and acknowledgement and Administrator only when Convergent is contracted to change monitoring configuration.
68. Remove the user's access separately from each customer when responsibility changes. Customer data remains isolated by explicit access grants and database row level security.

Location	Connection	What is exposed
Customer devices	Local connection from the site agent	No direct internet access is required
Customer agent machine	Outbound HTTPS TCP 443 to monitor.systemmatch.co.uk	Monitoring results only. No inbound port is opened
Integrator office	HTTPS sign in to monitor.systemmatch.co.uk	Only explicitly authorised customers and roles

Example

A customer site in the United States runs a SystemMatch agent on an always on machine inside its network. Fortinet permits that machine outbound HTTPS to monitor.systemmatch.co.uk. Convergent staff in London sign in to the cloud console and can view that customer alongside their other authorised customers. No VPN from Convergent to the customer and no inbound Fortinet rule are required.

Understand current product coverage

Status	Meaning	Examples
Live	Available and selectable now	Ping TCP HTTP Windows services disk CPU memory Event Viewer daily PDF reports and email alerts
Limited scope	Available only on the platform stated in the form	Linux software RAID through /proc/mdstat
Roadmap	Visible for planning but cannot be selected	SNMP interface monitoring deep SQL checks VMS vendor APIs hardware RAID SMART and backup job checks

Windows services disk CPU memory and Event Viewer are not partial. They are live local host checks. Event Viewer intentionally excludes message bodies as a privacy safeguard. RAID remains limited because hardware RAID needs vendor specific access. VMS features remain on the roadmap until each vendor API and licence has been agreed.

Customer troubleshooting

Symptom	What to check
One agent is Reporting and another is Late	If both were enrolled on one computer the reporting identity replaced the other. Keep the working agent unchanged and install the Late site's agent on a different machine or virtual machine
Agent is Late	The last report is overdue. Confirm the service is running, the machine is awake, and outbound HTTPS to monitor.systemmatch.co.uk is allowed
Agent is Offline	The reporting gap is longer. Check machine power, Windows service startup, internet access and any proxy or firewall change
Every private device is Critical	Confirm the production agent is online assigned to the same site and can reach those private addresses locally
Service check is UNKNOWN	Confirm the short service name and that the check is assigned to the Windows agent on that machine
Disk check shows the wrong volume	Enter the exact drive such as D:\ and confirm the agent runs on the computer that owns it
Event log is UNKNOWN	Confirm the channel exists and the agent service account can read it. Security can need extra permission
Test email works but no alert email	Create a new state transition and confirm the recipient list includes that severity
Device address changed	Reserve the address in DHCP or use a static address then update the device record

Windows checks for a Late agent

```
Get-Service SystemMatchAgent
& "C:\Program Files\SystemMatch\Agent\systemmatch-agent.exe" status
Restart-Service SystemMatchAgent
```

Wait up to two minutes after restarting. The agent normally reports every 30 seconds. Do not click Reissue token unless the service reports an authentication error. Reissuing cannot repair a stopped service, sleeping computer or blocked internet connection.

When asking for support include the site agent name device name check name time of the result and the request ID shown by the console. Never send passwords enrolment tokens or device credentials by ordinary email.