INFORMATION TECHNOLOGY REQUIREMENTS

Respond to each item below.

Software as a service:

1. **Applications must be hosted outside of the State Government Network (SGN).**
   Acknowledge Vendor's acceptance of this requirement:
   Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus acknowledges and accepts this requirement.

Securus SCP is a fully hosted centralized calling platform that operates independently of any state network. Securus will provide a fully private MPLS network to transport and process them without the use of any State government network.

2. **Provide the following information regarding your cloud provider:**
   - **A. Identity,**
   - **B. Location,**
   - **C. High availability zones,**
   - **D. Backup/disaster recovery features,**
   - **E. Secure access administration information.**

   Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Identity

Securus hosts the back-end equipment for our hosted, closed-based platforms in a carrier-class, commercial-grade, high-performance, managed data center built to the latest technology standards. This includes all hardware and software maintaining fraud controls, investigative features, user utilities, call/video processing, and communication event recording.

Location

Securus has long recognized the importance of securing customer data from loss due to local storage failure. To this end, Securus has invested heavily in modern IT infrastructure and in the IT staff to manage it. Each communication detail record (CDR), call recording, and video session recording is stored using Network Attached Storage array (NAS) technology in two separate places—a data center in Dallas, Texas, and a data center Atlanta, Georgia.

High-Availability Zones

Securus hosts our applications in two separate data centers that are in geographically diverse locations. Each Data Center has multiple, isolated availability zones or nodes. The incoming traffic is distributed between these nodes based on complex routing algorithms in the load balancer. Should a node in the data center fail, the load balancer routes service requests to the other available nodes. Our data centers and NAS storage infrastructure is monitored 24x7x365 by our Network Operations Center and

managed by a NAS analyst member of Securus' IT staff. Consequently, your data is always safe with Securus.

Backup/Disaster Recovery

Securus has designed and implemented a robust network architecture that provides for quick disaster recovery, minimizing downtime for the Securus platform and its customers. Securus has demonstrated its ability to recover efficiently under extreme circumstances, restoring service to our customers with no data loss.

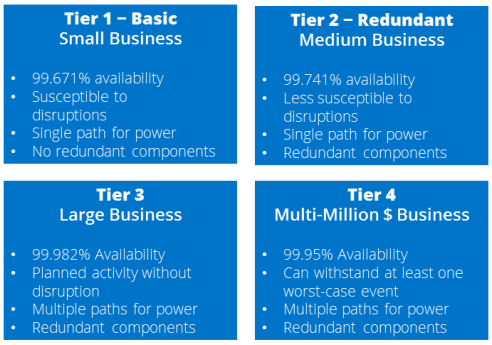
Risk Mitigation

Securus has implemented a platform and infrastructure designed to minimize potential outages and protect customer data. Multiple data centers, diverse network paths, redundant platform systems, and proactive monitoring mitigate the majority of risks.

Data Centers

Securus maintains a presence in two data centers in geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.95% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier IV (highest availability) data centers including:

- Ability to withstand a 96-hour power event
- Two-hour fire protection
- Multi-layer physical security
- Multiple power delivery paths.



TIA-942 Infrastructure standards for data centers
Telecommunications Industry Association

Also, Securus data centers have redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity. Securus data centers are staffed 24x7x365 for immediate physical assistance inside the data center.

Multiple checks ensure data center physical security, including guarded, photo-verified check-in; dual-door authentication (card and biometric); and a mantrap (interlocking door controller) at the data center suite entrance.

Redundancy

Redundancy is a key component of our hosted, cloud-based platforms. Our platforms run run on duplicate environments in separate data centers in Atlanta, Georgia, and Dallas, Texas. Each component has N+1 redundancy, meaning that a failure of any one component does not result in downtime because there is a backup available to resume its function. Securus has also designed

redundancy into all support systems, either through N+ 1 configuration, database clusters, virtual machines, load balancing, or other failover methods. All network transport has redundant network equipment and routing to allow traffic to reroute in the event of a failure.

Ourplatforms in Dallas and Atlanta were designed and built to the same specifications. This standardization allows re-homing of systems from their primary data center to an alternate data center in the event of a failure.

All circuits coming into Securus data centers use multiple diverse carriers, including the interconnections between data centers. In the event of a failure, traffic will reroute across a redundant circuit or path. In addition, Securus uses multiple carriers for incarcerant calls over our platforms. Calls to family and friends will immediately reroute upon failure of any carrier.

Securus uses industry-leading vendors for all platform and network hardware, including Dell, Cisco, Oracle, EMC, Big IP, and Intel. In addition to the redundancy designed into the platform and network, Securus also maintains a spare parts inventory onsite at each of our data centers to expedite repair of a failed component. Securus also maintains premium-level support contracts with each vendor that define stringent service level agreements in case of a failure.

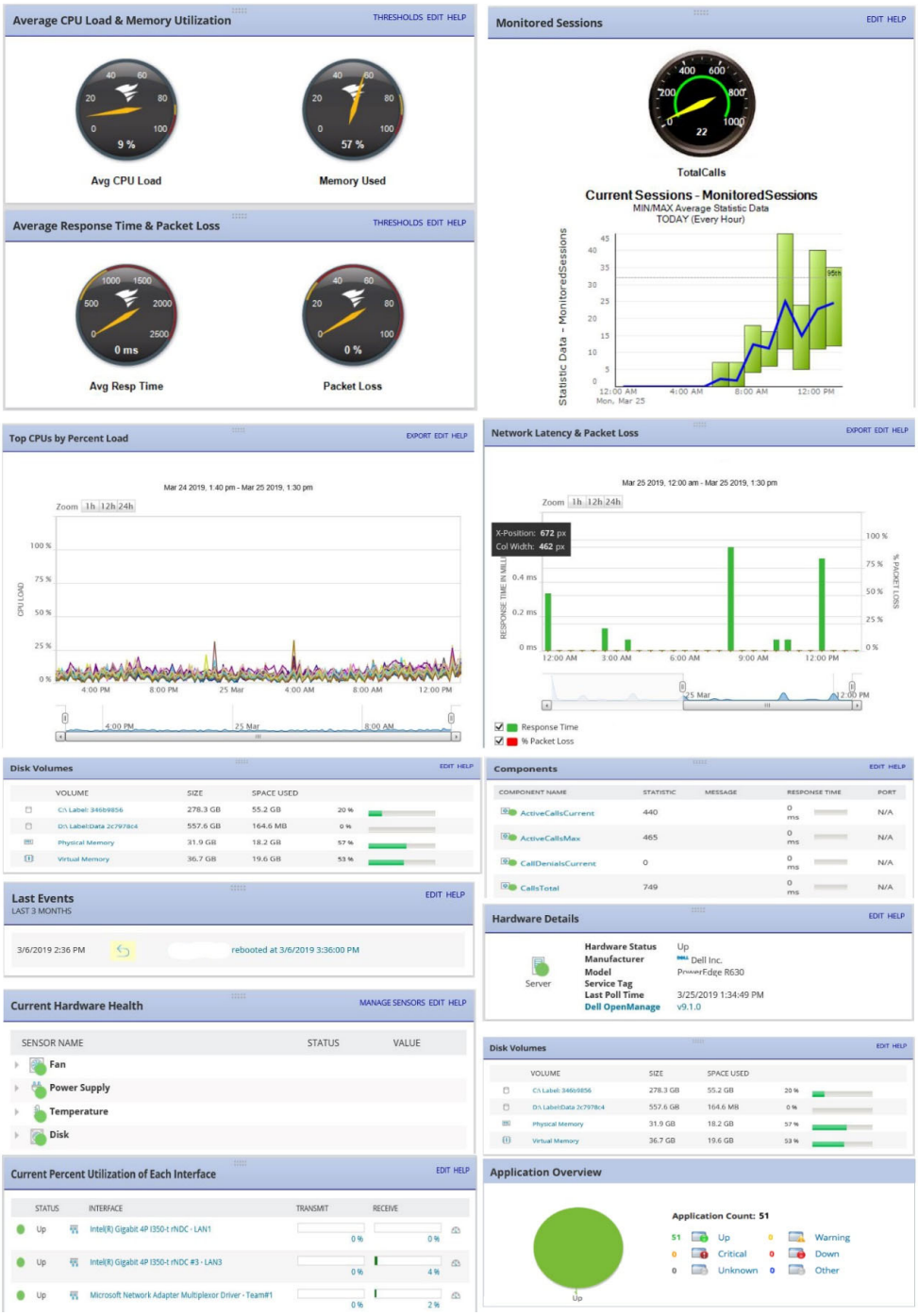
Securus maintains an inventory of spare parts for our facility-based components at our headquarters in Dallas, Texas, and has distribution agreements with multiple vendors to provide expedited national delivery service. The corporate headquarters maintains a standardized emergency recovery package of frequently used spare parts and equipment that will be available for shipment to support restoration efforts at our customer sites. Our technical field representatives located throughout the country also carry an inventory of the most commonly needed spare parts. With spare parts on board our service vehicles, most facility-based equipment malfunctions can be resolved with a single site visit.

Proactive Monitoring

Data Centers and Network

Securus continuously monitors all data centers, infrastructure components, platform systems, and incarcerant telephone systems (ITS) using the SolarWinds® suite of network performance monitors. The SolarWinds performance monitors are highly configurable to provide real-time monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring for all Securus systems, including NextGen SCP and all associated services, network, back-office systems, and data centers. The NOC proactively monitors these systems to ensure performance is optimal and uninterrupted. In addition to system- and network-level monitoring, the NOC also monitors real-time video surveillance and environmental alerts for our data centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.



SolarWinds® Typical Monitored System and Application Elements

Securus Primary Network Operations Center

Securus Network Operations Center

Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including integrated access devices (IADs), visitation phone monitoring (VPM) units, switches, and uninterrupted power supply (UPS) systems. The systems are polled every two minutes and their vital operating statistics sent every 10 minutes. Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, a Securus Field Technician is dispatched to the facility for on-site repair.

SolarWinds® Device Monitoring Example (Bandwidth & Network Latency)

In addition to real-time monitoring and alerting, Securus technical support also leverages the SolarWinds network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the technical support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

Restoration

Platform and Network

In the event of a disaster impacting our network, Securus immediately assembles a team of engineers to begin investigation and restoration of services. Securus maintains a schedule of on-call personnel for immediate response to service-impacting events and will also engage third party vendors, if required. If a state of emergency is declared, the Securus Business Continuity Plan will be activated.

Facility-Installed Systems

Securus prioritizes recovery of premise-based equipment by facility type and equipment location. Maximum-security institutions and institutions with high incarcerant phone usage receive priority. Prioritization also considers customer requirements and preferences. Securus has developed procedures and checklists to protect personnel and equipment in the event of an emergency situation. Securus will combine headquarters and field staff efforts to expedite service recovery wherever possible. Securus coordinates each checklist to ensure compliance with each facility's guidelines.

Securus has a field support department with more than 224 field service associates supported by a centralized field dispatch team. The Field Service Technicians (FST) are strategically located to support ongoing maintenance, as well as any disaster recovery situations. The FSTs are supported by senior technical support resources and engineering to expedite repairs and minimize customer downtime.

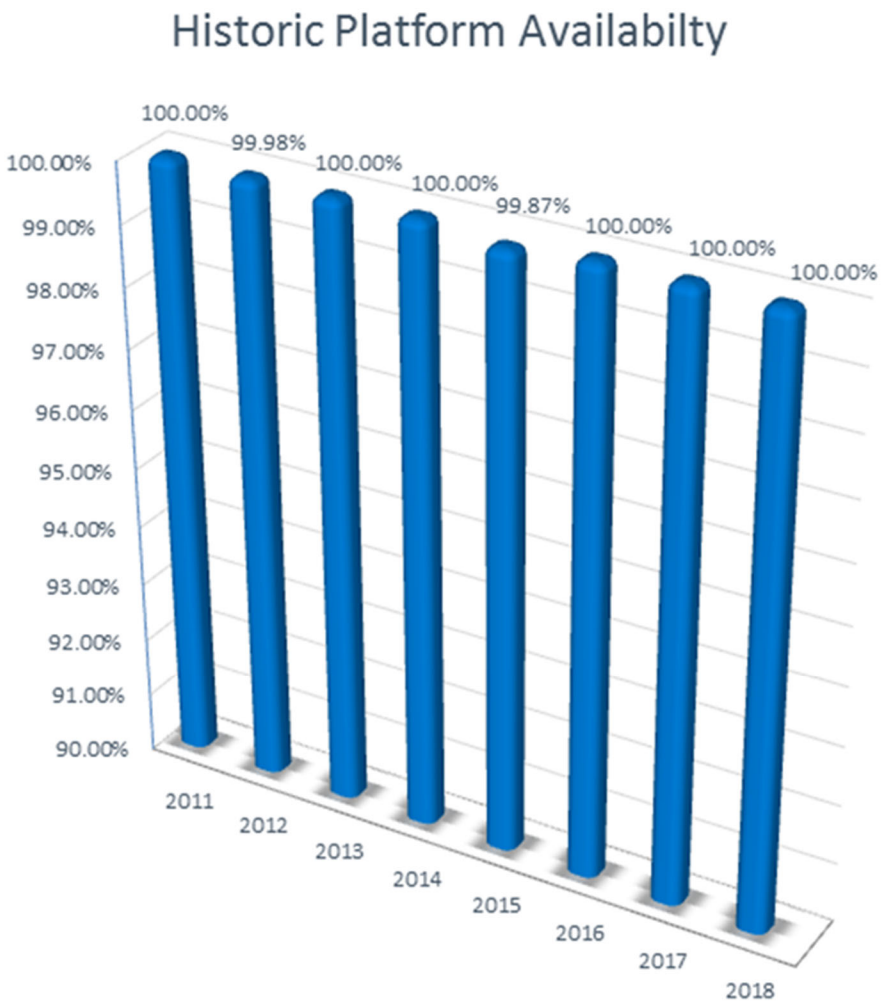
Reporting

Upon confirmation of a service-impacting event, the NOC will issue an internal service interruption report (SIR). The SIR will include the nature of the outage, impact to facilities, and estimated time of restoration, if known. Each incident is assigned an urgency level based on the level of customer impact.

Customer contact personnel receive SIRs, so they can communicate with customer facilities proactively or reactively as required by the facility. In addition, technical support may communicate a service-impacting event via a splash screen on the SCP user interface introductory page, whenever possible. Regular updates ensure that the information provided is always current. Securus executives also receive all SIRs, so they are aware of all customer-impacting events.

The NOC will issue a final SIR upon issue resolution. Securus investigates each incident and completes a root-cause analysis (RCA) following all service-impacting events. After the root cause is determined, Securus makes RCA documents available to customers upon request.

Performance for Secure Call Platform



The Secure Call Platform (SCP)'s reliability will extend to NextGen SCP, as they are based on the same centralized infrastructure, proven efficient and reliable over the past 12 years.

Our platform is one of the most stable platforms in the industry, with nearly perfect, 100% availability. Through design, proactive monitoring, and rapid-response procedures, Securus minimizes customer-impacting outages. Data storage with multiple layers of redundancy minimizes the risk of losing critical data and recordings.

When disasters strike, Securus responds quickly and methodically to ensure the fastest restoration of service possible. And we have been tested.

In the spring of 2015, the Dallas, Texas, area, home to two Securus data centers, was impacted by weeks of significant storms, resulting in 27 deaths and more than one billion dollars of property damage due to flooding. Early one morning, lighting struck a Securus data center, damaging

cooling units. Normally, this cooling would have been restored within minutes, but the roads leading to the data center were closed due to flooding, which caused a longer response time for service technicians. Securus' equipment rapidly overheated and began to fail. More than a quarter million dollars of components suffered fatal damage and needed replacement. Even with this once-in-a-lifetime series of compounding events**, calling services were restored the same day** for most facilities, and **there was no loss of customer data, investigative data, or recordings**.

Secure Access

Securus understands the importance of security, particularly in the corrections industry, and takes security concerns seriously.

Securus applies a high level of security to protect against cyber crimes. Applications that transmit data across public networks support SSL, Certs, and encryption. Cisco and Fortinet firewalls, used throughout the network to protect SCP and our customers, create DMZ networks. All servers, laptops and workstations require anti-virus and anti-spyware protection and the latest operating system patches. Securus supports both Bitdefender and Symantec anti-virus.

Data Security

Securus has a carrier-class data center that has some of the most comprehensive security measures in the telecommunications industry. Multiple layers of security control physical access to the Securus network facilities.

Security personnel maintain the following procedures for allowing entry into the data centers:

- Security personnel are on premise 24x7x365
- Cardkey reader (electronic badge) access for entry
- All persons having a business need to access company premises must carry identification badges at all times
- Man traps at each entry and exit point in the data center. Man traps use two sets of doors that both require electronic badge entry. The first set of doors must close before the second can open.

Access Procedures

All visitors, customers, contractors, and repair personnel must gain access from the security officer on duty.

Customers, contractors, repair personnel, maintenance personnel, and non-local employees can access buildings and critical areas only with an escort. Vendors may access buildings and critical areas only during working hours and also require an escort.

3. Applications must be fully maintained and supported by the Vendor. Describe how Vendor will meet this requirement including how Vendor will implement updates/upgrades and how often.
Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As a true turnkey provider, Securus fully maintains and supports the incarcerant communication applications we provide. Securus provides highly reliable service from initial system design and installation through ongoing maintenance and support. Our service and maintenance program includes integrated remote programming, diagnostics, downloading, and troubleshooting capabilities. Securus does not charge for maintenance, support, training, and repair of system software and equipment.

The local Securus service and account management team provide support 24 hours per day, seven days per week, and 365 days per year (24x7x365). The local team of Securus employees have demonstrated their dedication to the counties in the state of Washington.

The following in-house Securus teams work together to support our customers' technical needs:

- Your Securus account team

- Network Operations Center
- Technical Support Center
- Field services team

These teams ensure WA DOC's system is running at peak performance levels.

The Securus organizational structure has proven to deliver excellent service and technological innovation. Accountability, standards of excellence and leadership begin at the top of the organization with the Securus executive leadership team and filters down to each associate in the company. Each team member has a personal commitment to delivering outstanding customer care, service excellence and the creation of powerful applications and tools to meet our customers' needs. Our goal is to form long-term partnerships with our customers. We develop new applications to help customers run their business through a deep understanding of their needs.

Key Personnel for WA DOC

The principal personnel for WA DOC are experienced and qualified professionals that have an unparalleled combination of knowledge, skills, and technical proficiency. The key personnel assigned to the WA DOC program are:

Name	Title
Steve Cadwell	Account Sales Representative: Account Executive
Greg Levine	VP, Strategic Sales, JPay
Mario Ward	Director, Sales
Steve Viefhaus	VP, Sales
Amy Hewitt	Account Management, Manager, DOC (Service Manager)
Natasha Samuels	Account Manager, JPay
Lyon Dhanukdharrisingh	Manager, DOC Retention, Client Care, JPay
Dusty Finley	Sr. Implementation Project Manager

Field Service Technicians	
Field Service Technician	**Experience**
Dennis Shinpaugh	Field Services Manager
Jeff Ollar	Onsite FST at Pierce County, WA
Brandon Jenkins	Onsite FST at King County, WA
Kenneth Duhe	Rover FST
Russ Beecher	Rover FST.

John Phipps	Rover FST

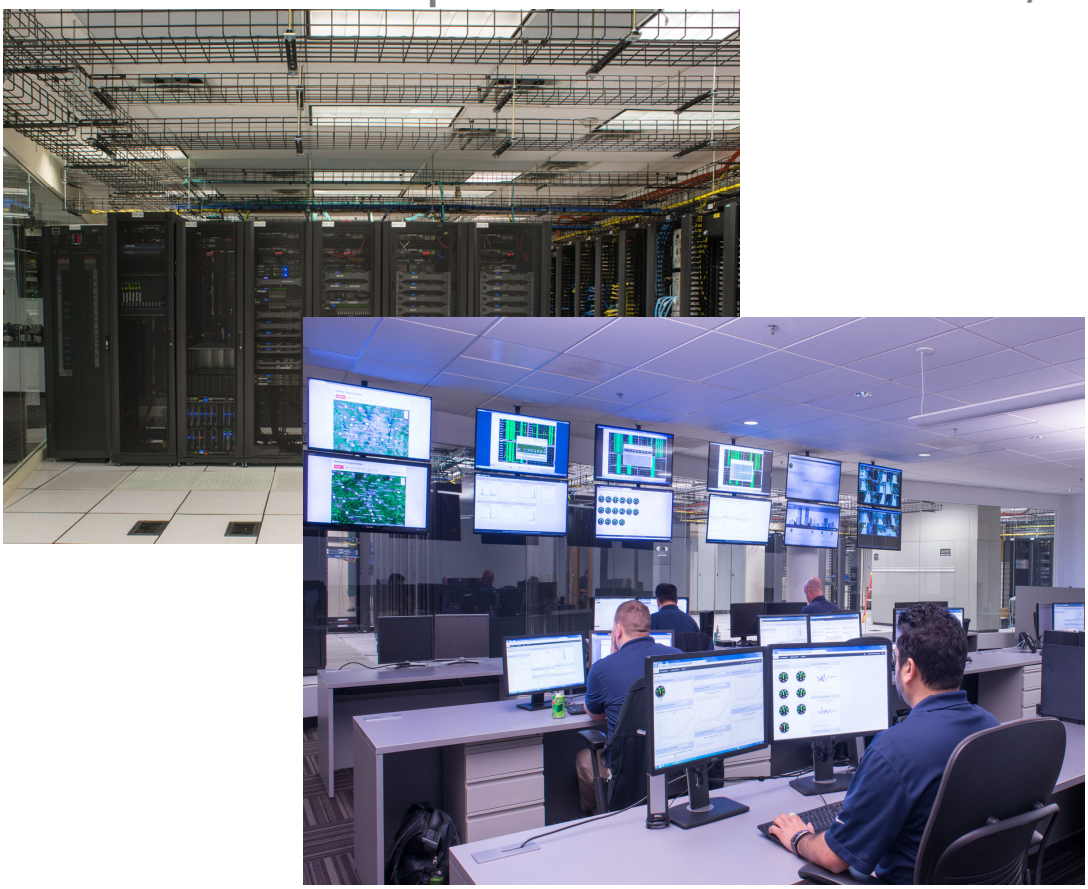
Network Operation Center

The Securus employees continuously monitor our platform from our Network Operations Center (NOC) at our headquarters in the Dallas, Texas, metro area. The NOC is staffed 24x7x365 by network experts certified in the systems and software used to monitor all NextGen SCP functions and equipment, as well as the associated network. The NOC maintains failure reports, service history, and other diagnostic information, which are available to the DOC when requested.

The NextGen SCP platform provides continuous online supervision and diagnostics—as well as offline system access—for advanced programming, diagnostics, troubleshooting, and call traffic analysis. The Securus service center personnel can access the NextGen SCP advanced diagnostics and program control for failure reports, service history, and other diagnostic information.

The NOC reports any actions required to prevent or repair any outages to each Securus employee supporting WA DOC. Securus will follow the DOC's protocols for communicating outages or repair actions in the unlikely event they occur.

Securus Network Operations Center in Dallas, TX



Premium Network Monitoring Capabilities

Securus proactively identifies potential system and network abnormalities through SolarWinds® suite of network performance monitors. This software allows Securus personnel to monitor all hardware, software and system metrics continuously.

Through network monitoring Securus can:

- **Proactively repair systems to prevent outages.** Many times corrections are made before a facility is aware of a problem. This means less downtime and increased system reliability for the facility.
- **Alert remote or on-site engineers of system threshold inconsistencies or alarms.** The NOC communicates with engineers through e-mail, short message service (SMS), or directly through a wireless phone to address the issue.
- **Receive real-time alerts when the system detects an error.** Monitoring identifies if network elements exceeded established thresholds and alerts Securus personnel of possible carrier network issues.
- **Ensure sufficient resources are in place.** The Securus capacity engineering team reviews call traffic volume reports and storage requirements throughout all systems to ensure sufficient network capacity.
- **Centrally monitor calling traffic to determine increases or decreases in the number of telephones.** With DOC agreement, the service and operations team will install additional telephones when required.

Remote Programming, Diagnostics, and Troubleshooting

The Securus NOC monitors the NextGen SCP platform and our network. The NOC can contact the Technical Support Center (TSC) if it determines that another level of technical support is needed to address an issue. This action could involve dispatching a Field Service Technician to a WA DOC facility.

Technical Support Center

In 2009, Securus made a strategic decision to centralize management of all technical support. Today, Securus provides superior customer service capabilities from a state-of-the-art technical support center located in the Dallas, Texas, metro area.

Approximately 50 technical professionals staff the Securus Technical Support Center (TSC) which handles approximately 8,000 inbound queries per month. The TSC provides a single-point-of-contact for Securus customers for issues ranging from minor maintenance issues to service outages. Clients can contact the TSC 24x7x365 by any of the following convenient methods:

- **Telephone** – 866-558-2323

- **E-Mail** – technicalsupport@securustech.net
- **Fax** – 800-368-3168
- **Web portal** - http://www.securustech.net/facility/Default.asp

The technical service center offers our clients:

- Technical support and field dispatch 24x7x365
- Fully trained staff of support professionals to answer calls
- Trained professionals to provide quick problem resolution and a higher level of customer service
- Service event tracking to drive resolutions
- Prioritized calls and analyzed reports to ensure achievement of Service Level Agreements
- Certified technicians to provide quick problem resolution
- System and individual site connectivity monitored 24x7x365

Securus technicians receive internal Securus certifications, based on our business and the products and services we support.

The Securus Field Services Team

The Securus Field Services organization is one of the largest in the incarcerant phone system industry. Our team consists of approximately 224 Field Service Technicians (FSTs) located throughout the United States, including five (5) in the State of Washington. Our teams have expanded based on our growing customer needs.

Our field services team installs and maintains incarcerant phone systems for approximately 2,600 facilities and a million incarcerants in 47 states. The Securus Field Operations Director manages three Regional Service Managers who possess more than 60 years of combined field service experience.

Field Service Technicians

Securus requires that all FSTs have an extensive telecommunications background and tests each applicant before employment. Additionally, FSTs receive extensive Securus training and certifications to support our product offerings.

FSTs respond to critical issues within four hours (or less if required by specific DOC requirements). The technician is required to follow a structured technical and management escalation process if they are unable to isolate the problem within four hours. Our integrated support model keeps our centralized technical support team engaged through problem resolution. FSTs and the technical support team have direct access to product and development engineers, enabling them to expedite repairs and minimize customer downtime.

Securus field service technicians maintain a working level of spare parts for minor repairs consisting of telephone sets, handsets, dials, and replacement circuit boards, either on-site or in their truck. If a technician does not have a required part, Securus will drop-ship the item to the site. Securus will ship counter-to-counter on the same day in critical situations.

Field Service Manager

In addition to FSTs, Securus customers are supported by field service managers who:

- Conduct remote visits via phone bimonthly. Based on information obtained from call, a trouble ticket may be opened
- Work with the account team quarterly to evaluate contract progress with the DOC
- Provide the facility with applicable site information that assists them based on the account profile
- Monitor ticket traffic
- Resolve escalation issues, as needed.

Each field service manager possesses the skills required to perform the duties of the field service technician and can provide additional or backup support as needed.

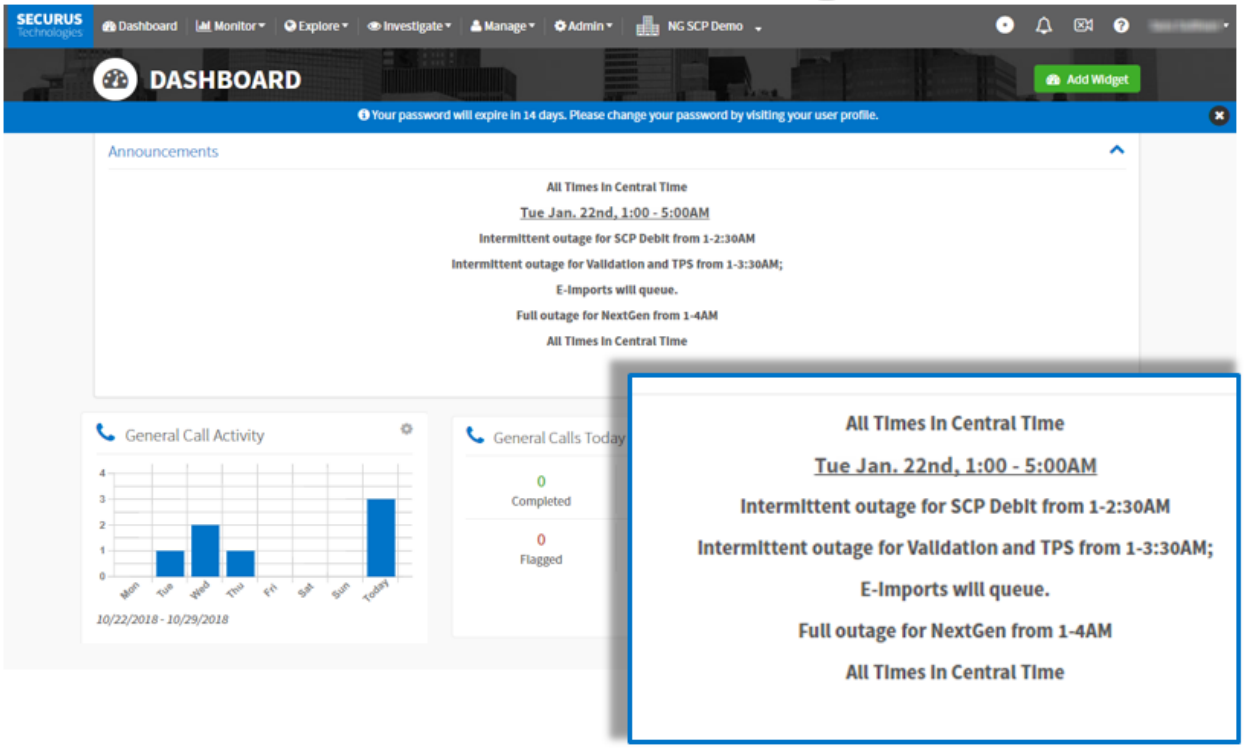
Software Upgrades

We recognize that the challenges you and your officers face every day never stop evolving. When we designed our centralized platform, one of our chief objectives was deploying a system that provided upgrades to all customers at regular intervals with no downtime. Securus provides upgrades to all of our customers three to four times annually through a proven and tested after-hours process that allows all sites to immediately realize the benefits each upgrade. Our system delivers proven features driven by input from the most recognized corrections and law enforcement agencies in the nation.

Maintenance events are preceded by an announcement displayed at login notifying the facility of the upcoming upgrade and new features are announced to customers prior to implementation. These system updates are more than simple changes. They provide meaningful features and new capabilities, which drive greater officer and community safety, staff efficiency and improved investigative response times.

The following image shows the announcement widget, which appears for all users on the NextGen SCP dashboard, and notifies users of upcoming maintenance and upgrades.

Announcement Widget



Tablet Upgrades

Our tablet systems can receive patches and upgrades on a daily or weekly basis depending upon need or development. Any new features are discussed with our clients prior to implementation.

4. All software licensing will be the responsibility of the Vendor. Describe how the proposed system will meet this requirement including a list of software for which the Vendor anticipates it will be licensing for this project and the specifications of that software.
Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As a turnkey provider, Securus will be responsible for all applicable software licensing.

Securus will grant the State a personal, non-exclusive, non-transferable license to access and use certain proprietary computer software products and materials in connection with the Applications (the "Software"). The Software includes any upgrades, modifications, updates, and additions to existing features that may be implemented. Securus will also provide or pre-install third-party software required to access the Software, such as the Google Chrome® web browser required to access the NextGen SCP system.

The following software programs will be licensed via third-party for all Securus-provided workstations:

- Microsoft Silverlight 4.0 or newer
- Microsoft .NET Framework 4
- Adobe Reader 9.5 or newer
- Microsoft Office Excel Viewer
- Quick Time 7 or newer
- Windows Media Player
- Antivirus
- WinZip or other zip utility

IT Hardware Support:

1. **All IT hardware (including tablets, phones, routers, etc.) must be provided and fully supported by the Vendor. Acknowledge Vendor's acceptance of this requirement**
   Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus acknowledges and accepts this requirement.

2. **Provide emergency hardware support contact information.**
   Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

In the event of an emergency hardware situation, Securus provides various contacts to get support. Our goal is to make it as easy as possible for WA DOC personnel to communicate with us. WA DOC will be provided with the following:

- An Account Management Team that will serve as a dedicated points of contact for WA DOC
- A Technical Support Center available 24x7x365
- Onsite Field Service Technicians at two WA DOC facilities

Account Management Team

WA DOC will have an assigned and dedicated account management team, which includes not only the sales and support staff, but also Account Managers assigned specifically to WA DOC. In addition to Natasha Samuels, WA DOC's current Account Manager for JPay services, WA DOC will be assigned an account manager for Securus ITS, VVS, and associated services, who will be responsible for product training, monitoring system and product usage, proactive account support, account reviews, and reactive account support in order to ensure quality of service. Upon award WA DOC will be provided full contact information for your account managers.

Technical Support

WA DOC can always contact the Securus Technical Support Center (TSC) to ensure prompt problem resolution. The Securus TSC serves is available **24 hours a day, seven days a week, 365 days per year.** There are three ways to contact the TSC:

- Telephone: 866-558-2323
- E-Mail: technicalsupport@securustech.net
- Fax: 800-368-3168

The TSC uses a call distribution system to manage the flow of inbound customer calls automatically routing calls directly to our support technicians in a skills-based, platform specific manner. Securus establishes response times and service level agreements that accomplish our objective of providing timely resolution to each request.

Technicians assign each service request one of three initial priority levels, each with resolution and escalation timelines. The TSC uses an event tracking system that logs, tracks, manages and assures appropriate response to all service requests. The service request generates a trouble ticket with priority level assignment that drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem and either resolves the problem or engages an appropriate party for problem resolution. The TSC retains ownership of all service requests and is responsible for the escalation and update functions.

On-Site Field Service Technicians

We currently have five field service technicians located in Washington state. We can provide onsite field service technicians dedicated to WA DOC if necessary. We suggest discussion the DOC's needs for this at our upcoming presentation on October 28.

3. The solution must have automatic problem reporting capabilities notifying the Vendor of problems with the system. Describe how Vendor will meet this requirement and describe how and when Vendor will notify DOC.
Vendor's response:

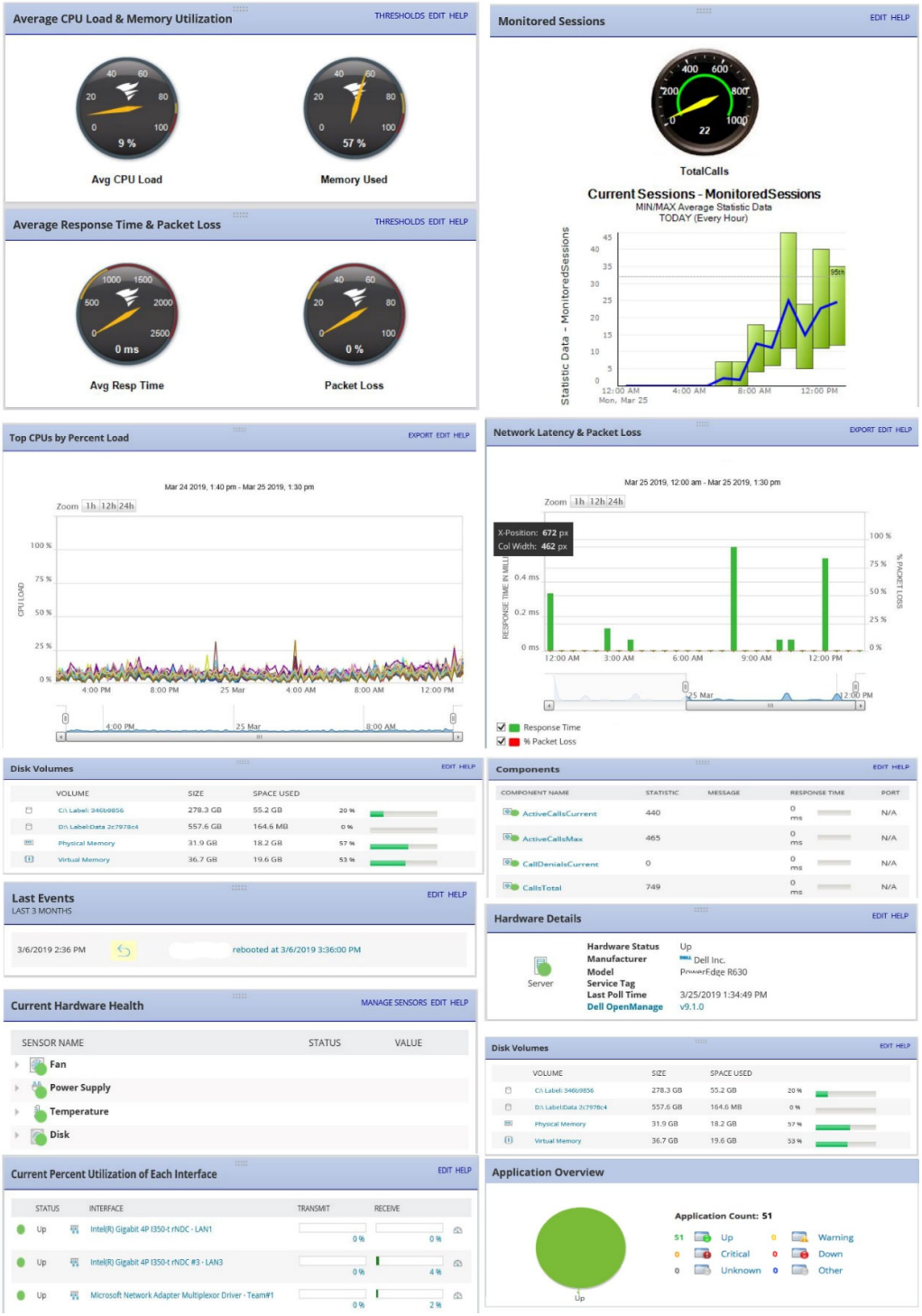
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus continuously monitors all data centers, infrastructure components, platform systems, and communications services using the SolarWinds® suite of network performance monitors. The SolarWinds® performance monitors are highly configurable to provide real-time monitoring, event notification, alert history and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring for all Securus systems, including the NextGen Secure Communications Platforms™ (NextGenSCP™), network, back-office systems, and data centers. The NOC proactively monitors these systems to ensure performance is optimal and uninterrupted. In addition to system and network-level monitoring,

the NOC also monitors real-time video surveillance and environmental alerts for our data centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.

SolarWinds® Typical Monitored Application Elements



Securus Primary Network Operations Center

Securus Network Operations Center

Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including Integrated Access Devices (IADs), Visitation Phone Monitoring (VPM) units, switches, and Uninterrupted Power Supply (UPS) systems. The systems are polled every two minutes to ensure proper operation, and their vital operating statistics sent every 10 minutes. Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, a Securus Field Technician is dispatched to the facility for on-site repair.

SolarWinds® Facility Monitoring Example

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the SolarWinds® network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

Infrastructure Inspections

System Administrators make scheduled inspections of all systems and routinely perform preventive maintenance and software enhancements as directed by a Production Change Control steering group. Additionally, change control practices have been reviewed and are compliant with Sarbanes-Oxley.

NOC Monitoring of Kiosks

A team of engineers in our Network Operations Center (NOC) monitors and provides Level 1 support for each installed kiosk. The kiosks report to our central servers every ten minutes on usage, network speed, connectivity, and any errors or issues encountered. If a kiosk fails to check-in or reports any issues, our central monitoring tool alerts the NOC engineers who troubleshoot the kiosk remotely.

NOC engineers can remotely access each kiosk and run diagnostics to determine and correct software issues. Resolution can be as simple as remotely restarting the application or as extensive as running full diagnostics on all software and hardware components. Most issues are detected and repaired before incarcerants or facility staff are aware of a potential problem.

At times, the underlying root cause is either network connectivity or hardware failure. If the issue is related to network failure, NOC engineers can remotely diagnose and correct most issues; otherwise, they dispatch a local field engineer to address the issue and if necessary, replace a failed component.

If NOC engineers are not able to address a particular software issue, they escalate it to a team providing application support (Level 2) who determine if the issue is a misconfiguration or an actual software bug. A misconfiguration, once identified, is addressed within a few minutes. A software bug is prioritized and addressed by the application support team. A software fix can be available in a few hours or a few days depending on its severity.

JPay releases software upgrades every few weeks, in which an automated process upgrades every kiosk to ensure all locations are running the same software build. Metrics collected from the kiosks and our central monitoring tool are combined into a set of reports that enable us to track the health of each kiosk. In addition, we mine this data to determine patterns in issues encountered and types of failures so we can continually improve our software, hardware, and processes.

4. Provide all hardware specifications.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will add additional hardware as needed once site surveys are completed. Please See Exhibit A – Hardware Specifications for more detail.

NG Secure Communications Platform (NG SCP)

Item	Make/Model
Phones	Wintel 7010 Stainless Steel, 18" handset Wintel 7010 Stainless Steel, 32" handset
TTY Phones	Ultratec TDD, Minicom IV Ultratec Superprint 4425
CapTel Phones	Ultratec CapTel Phone Model 840
VRS Terminals	sPhone XL, 88000-90050-01
Routers	Adtran Netvanta 3140
Servers	NSD2, TCS 036-01664-001,
Switches	Adtran, Netvanta 1534 Adtran, Dual Mounting Tray Adtran, Netvanta 1534P
Wireless Access Points	Ruckus Zoneflex R600
UPS	Eaton 3S750
Surge Protectors	Panamax Tower Max 4KSU Tripp Litte, DNET1, Type RJ45 Protector, ITW Linx, CAT 6 64488 V-Line, Shelf, #SB-745S1919 SFB
Workstation	Dell Optiplex 3050
PC Monitor and Speaker	22" LED Monitor, Dell P2217H Dell AX210 Speakers

Terminal Used for VVS, eMesasging and other Kiosk Services

Item	Make/Model
Kiosks	sPhone XL sPhone XL2

Tablets

Item	Make/Model
Tablets	JPay6 – Pre-loaded 7 inch tablet
Charging Stations	Tripp-lite CSC64MICROUSB

Data Ownership

1. **All DOC data removed from a DOC Facility will remain the sole property of DOC. Backup and disaster recovery copies must be returned to DOC upon expiration or termination of the contract. Acknowledge Vendor's acceptance of this requirement.**
   Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus acknowledges and accepts this requirement.

2. **Describe Vendor's proposed processes for data transfers between DOC and the Vendor including the type of encryption used for data in transit.**
   Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Access to all Securus server information is done through HTTPS (HTTP over TLS). HTTPS is the use of Transport Layer Security (TLS) as a sub-layer under regular HTTP application layering. The NextGen SCP dashboard encrypts and decrypts user page requests, as well as the pages that are returned by the Web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks (an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other). Applications that transmit data across public networks support TLS, Certs, and encryption. Sensitive data is encrypted both at rest and in motion. Securus provides supporting TLS encryption at the application network layer. All web sessions and services are executed via HTTPS using AES 256 encryption. Securus uses both GoDaddy and Entrust SSL certificates for external connections and Microsoft Active Directory Certificate Services for internal SSL connections where needed.

3. **All data, when transferred in or out of the system must use Secure File Transport (SFT) protocol. Which SFT provider will Vendor use?**
   Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has proven experience with Integration. Securus currently integrates with more than 110 different vendors worldwide and more than 60 independent, facility-owned systems and shared databases.

Securus has a dedicated integration department that integrates various systems and products in the corrections environment. This dedicated integration department allows Securus to deliver fast and flexible solutions for our customers. The Securus technology has the flexibility to work with

facility-owned systems, offender management system (OMS), commissary, banking, and kiosk vendors. Securus will fully cooperate with your facility and your vendors to automate systems.

The most common technologies Securus uses include SOAP Web Services, HTTP, SFTP push or pull of files in any textual format, JSON, XML-RPC, and TCP Sockets. All of these methods integrate over secure connections.

Securus can modify your data format for migration into our platform, without costly code modifications. Securus integration engineers consult with facilities' IT departments or system providers to determine the best integration strategy for each specific application.

Securus Integration Process

Securus' dedicated integration team designs, develops, tests, and implements all custom integrations with corrections industry vendors and banking systems to deliver fast and flexible solutions for our customers. This process is part of the overall project plan for the installation of the NextGen Secure Communications Platform™ (NextGen SCP™). Major milestones include:

- Collect preliminary needs/requirements
- Contract signed
- Finalized requirements document
- Approved scope statement
- Finalize design document
- Schedule customer implementation
- Develop custom integration solution
- Test custom integration solution
- Implement custom integration solution
- Customer approval and sign-off

OMS Integration

The Securus NextGen SCP can be integrated with a facility's OMS or commissary system so that the incarcerant PINs are automatically transferred, activated, and deactivated based on the incarcerant's status. If an incarcerant is released, the incarcerant's PIN is stored and can be reactivated along with call detail or visitation records and incarcerant call or visitation recordings if the incarcerant returns to the facility.

The following list identifies fields that can be automatically populated in NextGen SCP from an OMS or commissary integration:

- **First Name** – Incarcerant's first name
- **Middle Name** – Incarcerant's middle name
- **Last Name** – Incarcerant's last name

- **Birth Date** – Incarcerant's date of birth
- **Social Security Number (SSN)** – Incarcerant social security number
- **Account Number** – Incarcerant's jail ID, jacket ID, or docket number, to be used as the NextGen SCP incarcerant custody account number. Any number permanently assigned to an incarcerant that does not change if they are released and booked back into the facility.
- **PIN** – 4- to16-digit code used by the incarcerant to place phone calls.
- **Activate Date** – Date in which the incarcerant account became active in the system
- **Book Date** – Date that the incarcerant entered the facility
- **Gender** – Incarcerant's gender
- **Housing** – Location of the incarcerant
- **Race** – Incarcerant's race
- **Alert Level** – Typically used for security status such as maximum, minimum, low risk, and death row
- **Max Call Duration** – Call duration applied to each phone call placed by this incarcerant
- **Three-Way Detection** – Setting to enable or disable three-way call detection for this incarcerant
- **Language Preference** – Language in which the incarcerant speaks for reporting purposes (does not dictate the language of phone prompts)
- **Suspended** – Allows or prevents the incarcerant from placing calls
- **Suspend Start Date** – Start date of calling privileges suspension
- **Suspend End Date** – End date of calling privileges suspension

Securus currently integrates with more than 110 vendors worldwide, including:

ABL Management, Inc.	FirsTech	PTS Solutions
Aramark	FSG Software	Sleuth
Archonix	Genesis	Southern Software
Beacon Software Solutions	Global Software	Spillman
Canteen	Golden Eagle	Stellar
CBM	Guarded Exchange	Stewart Commissary
CenturyLink	Huber & Associates	Sungard/OSSI
Cirqular/SecurManage	ID Networks	SunRidge Systems
CIS	Intellitech	Swanson

Cisco	Intergraph	Synergistics Software Inc.
Compass Group	J-CORR Technologies/Abbey Group	Syscon
Correctional Food Services	Justice Data Solutions	TAC-10
Correctional Food Services/ITF	Justice Software	Tech Friends
Cottrell Consulting	Keefe	Telerus
CTS America	Kimble	Telus
Cushing Technologies	Lawrence and Associates	Text and Data/JAMIN
D&D Vending	M&M Micro	Tiburon
Digitech/Jail Tracker	MoneyGram	Tiger
DSI/ITI	Netdata	Touchpay
DSSI	New World	TriTech Software Systems
Eagle Advantage	Northland IT Solutions	Trinity Services Group
edocTec	Northpoint Institute, Inc.	Turnkey
EForce	Omni	Tyler Technologies
E-Justice/Crime Cog	Premier Supply Link	UniSys
Embarq	Prevatek	VisionAir
Emergitech	Primonics	Western Union
EnRoute 911	Pro Phoenix	Windspeed Software
EZ Card and Kiosk	PTS	Zuercher Technologies

4) Data residing on the system must be stored as encryption at rest. Describe how Vendor will meet this requirement including the type of encryption to be used.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus encrypts data at rest and in motion. Additionally, sensitive data such as social security numbers and passwords are stored within encrypted databases. We use AES 256 encryption for all communication between the site and the Data Center.

Access to all Securus server information is done through HTTPS (HTTP over TLS). HTTPS is the use of Transport Layer Security (TLS) as a sub-layer under regular HTTP application layering. The NextGen SCP dashboard encrypts and decrypts user page requests, as well as the pages that are

returned by the Web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks (an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other). Applications that transmit data across public networks support TLS, Certs, and encryption. Securus uses both GoDaddy and Entrust SSL certificates for external connections and Microsoft Active Directory Certificate Services for internal SSL connections where needed.

5. **Successful Vendors need to enter into a Data Sharing Agreement with DOC. Acknowledge Vendor's acceptance of this requirement.**
Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus acknowledges and accepts this requirement.

6. **Provide hardware currency specifications for kiosks, servers, portable tablets, etc. The expectation is that the hardware deployed at transition time will be current with latest industry hardware with no more than one year of age.**
Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will add additional hardware as needed once site surveys are completed. Please See Exhibit A – Hardware Specifications for more detail.

NG Secure Communications Platform (NG SCP)

Item	Make/Model
Phones	Wintel 7010 Stainless Steel, 18" handset Wintel 7010 Stainless Steel, 32" handset
TTY Phones	Ultratec TDD, Minicom IV Ultratec Superprint 4425
CapTel Phones	Ultratec CapTel Phone Model 840
VRS Terminals	Primonics sPhone XL, 88000-90050-01
Routers	Adtran Netvanta 3140
Servers	NSD2, TCS 036-01664-001,
Switches	Adtran, Netvanta 1534 Adtran, Dual Mounting Tray Adtran, Netvanta 1534P
Wireless Access Points	Ruckus Zoneflex R600

UPS	Eaton 3S750
Surge Protectors	Panamax Tower Max 4KSU Tripp Litte, DNET1, Type RJ45 Protector, ITW Linx, CAT 6 64488 V-Line, Shelf, #SB-745S1919 SFB
Workstation	Dell Optiplex 3050
PC Monitor and Speaker	22" LED Monitor, Dell P2217H Dell AX210 Speakers

Terminal Used for VVS, eMesasging and other Kiosk Services

Item	Make/Model
Kiosks	sPhone XL sPhone XL2

Tablets

Item	Make/Model
Tablets	JPay6 – Pre-loaded 7 inch tablet
Charging Stations	Tripp-lite CSC64MICROUSB

Other

1. **On a scale of 1 to 10 where 1 = extensive custom development and 10 = no custom development, based on DOC requirements how much custom development is needed for Vendor's product to meet the department's needs?**
   Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The proposed products and services which Securus has presented here generally represent a 9 to ten grading under the custom develop scale represented above by WA DOC.

2. **If custom development is needed, Vendor may not rely on DOC resources to accomplish the custom development. Acknowledge Vendor's acceptance of this requirement.**
   Vendor's response

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus acknowledges and accepts this requirement. As indicated above and as currently proposed, the majority of custom products will not require custom development but, to the limited extent customer development will be necessary, we will not rely on DOC resources to do so.

3. The system must have the ability by DOC to manage access control including step-by-step instructions. Describe how Vendor will meet this requirement.
Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Upon implementation we will be working with the WA DOC to identify system access to all component functions. So initially upon installation the systems are configured according to DOC policy and decisions. Ongoing access control is achieved through the user administrators function based up access permission granted and can be changed at any time by authorized users.

Both the NextGen SCP system and the JPay Facility System use role-based access to determine user permissions.

NextGen SCP Security Roles

NextGen Secure Communications Platform™ (NextGen SCP™) uses security roles to determine user permissions. WA DOC will be able to manage access control through the Security Roles in the user interface. This allows authorized WA DOC users to upgrade the access and security of users, including:

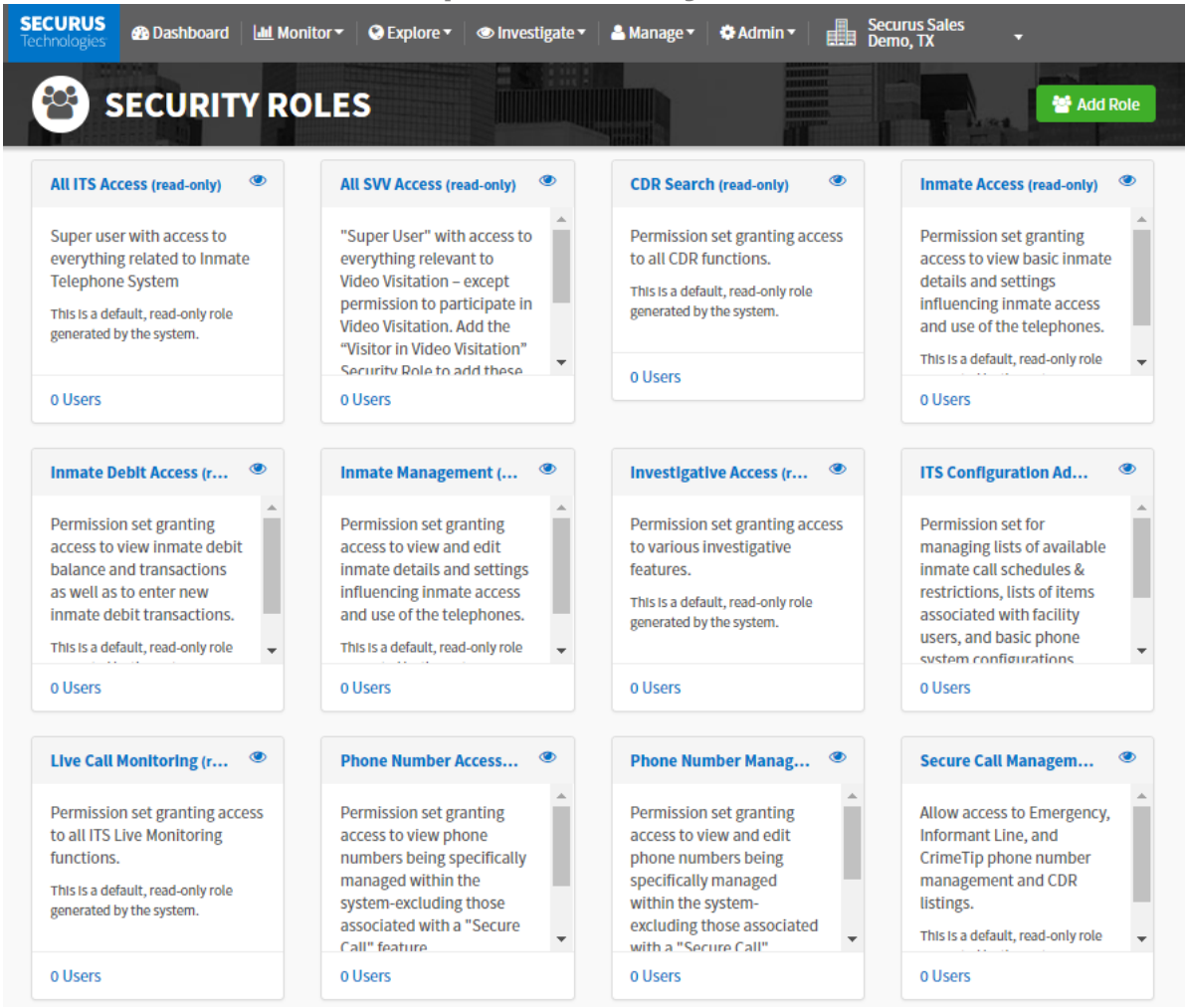
- Provide users with only the information they need to see, edit, manage or interact
- Easily craft custom task-based permissions for users
- Protect your facility access with required strong passwords and enforced regular password updating
- Provide facility affiliated personnel with access to video visitation

Security Roles define what actions a user can and cannot do within the system. NextGen SCP contains default security roles, identified by the eyeball ( ) icon. While these predefined roles cannot be modified, they cover many customers' needs for granting access and denial rights based on common job functions.

NextGen SCP provides more options for WA DOC to further customize access privileges by allowing authorized administrative users to either create a new user-defined role or create a new role using an existing role as a base and further modifying it. The user-defined role can be customized to meet WA DOC's specific needs when a default role does not. These roles are identified by the pencil ( ) icon.

In addition, the WA DOC administrator can assign multiple roles to a user to tailor their access to exactly what is needed. This provides virtually unlimited options for customizing users' access.

Sample Security Roles



Password Policies

NextGen SCP uses strong passwords that require users to update passwords regularly. Passwords must comply with the following rules:

- 8 – 12 characters
- No spaces
- Cannot contain the user's first or last name

At least three of the following types of characters must be used:

- English uppercase letter
- English lowercase letter
- At least one number
- At least one special character

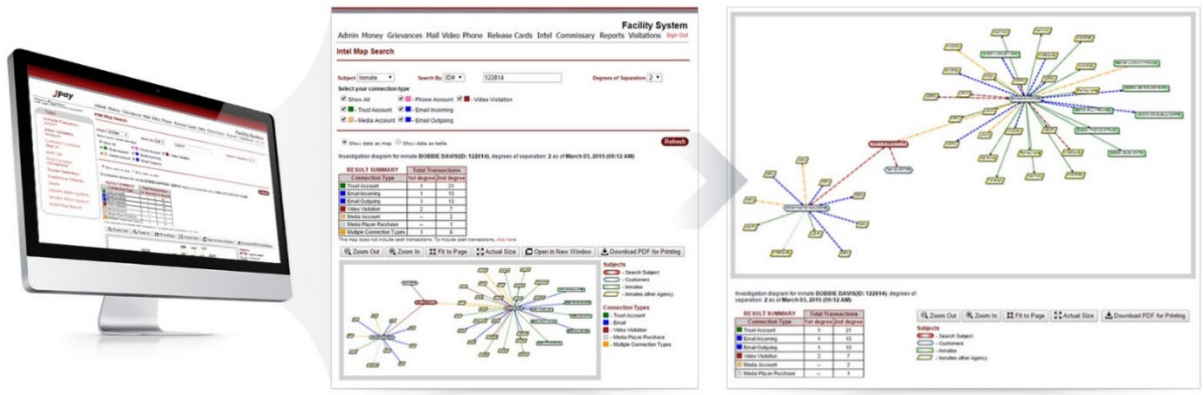
Passwords can be configured by location, days to expire, and even the number of password cycles before password reuse. Additional configuration options include reminders for password expiration and minutes of allowable inactivity before session timeout.

The “Forgot Your Password?” feature available from the login screen offers online support for users who have forgotten their password or for those who did not change their password before expiration. System security requires users to provide the correct answers to preset questions before their password can is reset. Once a new password is created, NextGen SCP emails confirmation to the address linked to the user ID.

JPay Facility System

The backbone for management of all JPay services is a secure web portal called the Facility System. DOC staff members use it to manage deposits, review transaction history, and access powerful link analysis tools to recognize customer and incarcerant relationships. The Facility System provides reports and detailed transactions for all payments and batches. It also enables feature-rich management of release cards, email, video visitation, VideoGrams, and music downloads. It is accessible from any computer or mobile device with an internet connection.

The Facility System - a comprehensive Intel system



Role-Based Access

The Facility System uses two-factor authentication for DOC users, making access both role-based and limited by facility. The DOC determines which staffers have access to the Facility System and administers access through discrete user groups. This feature, for example, can limit mailroom staff’s access to those aspects of the Facility System that deal specifically with electronic messaging, while accounting personnel only access electronic funds transmission.

JPay’s Facility System constantly evolves to meet the needs of client agencies. The rules that can be applied to both user access as well as service control and reporting is comprehensive. These business rules are configurable according to each DOC’s reporting and management needs.

User rights are customized for each staff member, though individual staff members with similar rights can be granted identical levels of access by being added to a user group. When creating a

user, authorized staff can add that user to a group without having to individually recreate permission sets for that user. Even if a user is assigned to a user group, administrators can tailor the user's permission level and access.

Reporting

DOC facility staff can use the Facility System to access transaction details for all payments and release cards. Users can generate standard and ad hoc reports on a per-facility basis or statewide. Users can also export reports to the Microsoft® Office suite for advanced sorting and analysis and save them in PDF format.

Money Transfer Reports

Daily Batch Report

This report displays the total transactions and dollar amount deposited to the DOC or each individual facility daily. The user can drill down to obtain detailed transaction information.

Weekly Deposit Report

This report allows facility staff to easily search for deposit information for any range of time. The report displays both the transaction volume and dollar amount and is useful for reviewing historical data.

Monthly Recap Report

This report summarizes the monthly totals per facility for all JPay services deployed. In the example shown below, the facility uses JPay's money and mail products.

Release Card Reports

Summary Reports

The Facility System gives users access to reports that detail cards issued, cards reloaded and cards modified or voided. Reports can be viewed for one or multiple facilities or statewide.

Authorized staff can click on any report to see the details of issued, voided, reloaded and modified cards. All reports can be drilled down or exported to Excel for additional analysis.

The following information is contained on each report:

- RPID number, incarcerant name, ID, and DOB
- Date the card was issued
- Username of staff member who issued the card
- Amount that was initially transferred to the card
- Amount that was added to or subtracted from the card

EXHIBIT A – HARDWARE SPECIFICATIONS

Mini Stainless Steel 7010SS

- Built-in user controlled volume "LOUD" button for ADA mandated volume control (must be user-controlled volume amplification AND volume must be reset to normal with on-hook to meet ADA requirements).
- Heavy duty 14 gauge brushed stainless steel provides rugged vandal resistant telephone housing designed for inmate use.
- Confidencer technology, built into every dial, filters out background noise at the user's location, allowing better sound to the called party.
- All-in-one electronic dial features modular incoming line and handset connections for quick maintenance. Carbon (HS) and DuraClear (DURA) Handsets have separate 4-pin connections.
- Heavy chrome metal keypad bezel, buttons, and hookswitch lever withstand abuse and vandalism.
- Armored handset cord is equipped with a steel lanyard (1000# pull strength) and secured with a 14 gauge retainer bracket for maximum vandal resistance.
- Handset has sealed transmitter and receiver caps, suitable for heavy use and abuse locations.
- Pin-in-head security screws minimize tampering.
- Hearing aid compatible and FCC registered US:1DATE05BITC-254, IC:3267A-ITC254.

ACCESSORIES:

- Handset length and style of your choice, choose carbon or DuraClear
- Standard 178A Backboard for mounting
- Adaptor Plate for mounting Mini Phones to 178A Blackboards and pedestals
- Conduit Backboard with two (2) or (4) entry positions
- Standard Flush Mount Pedestal
- Adjustable Pedestal
- 4 Wheel Rollcart

Wintel®
A Division of Independent Technologies, Inc.
1051 Bennett Drive, Suite 101 • Longwood, FL 32750
407.834.1188 • Fax 407.830.1050 • 800.264.8889
www.wintelphones.com

Ultratec

THE WORLDWIDE LEADER IN TEXT TELECOMMUNICATIONS

Minicom IV

This basic TTY is affordable and easy to use. It has an easy-touch keyboard with a bright, tilted 20-character display for hours of comfortable use. Minicom IV includes a printer port to connect an external printer. Turbo Code lets you enjoy "real-time" conversations with other Turbo Code TTYs. Auto ID lets everyone you call know you are using a TTY. Available options include an extended warranty, a dust cover and a soft carrying case. For basic communication features in a reliable TTY, Minicom IV is right for you.

Minicom IV

- Turbo Code® and Auto ID™
- Convenient GA/SK keys
- Printer port to connect to your external printer
- 20-character display
- 43-key, 4-row keyboard
- Rechargeable batteries and AC adapter included
- Baudot code (45.5/50 baud rate)

KROWN MANUFACTURING, INC.

PortaView 20 Junior

Krown-TDDs PortaView PV20 Junior delivers superior communications for all your telephone calls!

Krown-TTYs reputation of providing the most technologically advanced and highest quality TDDs at affordable prices is reflected in the PortaView 20 Jr. feature for feature, the PV20 Junior is an excellent value when compared with other ttys available today. It utilizes the same degree of quality engineering to provide years of the highest reliability and outstanding performance.

FEATURES

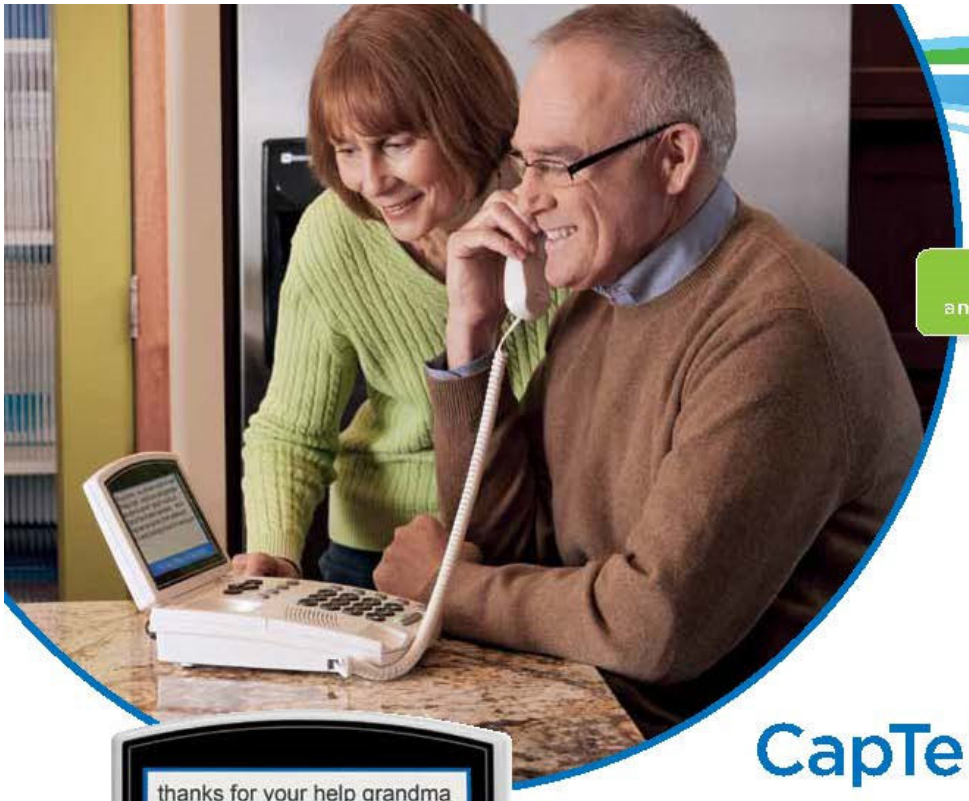
- 4-Row Keyboard
- 20 Character Display
- Heavy-Duty Rechargeable Battery
- Rugged Injection-Molded Case
- Acoustic cups to fit Round and Square Handset
- Pre-recorded greeting messages
- GA - SK combination keys for easy typing
- Physical Dimension
  Weight: 2.7 lbs (1.36 kg) with batteries
  Size: W 10" (25.4 cm), L 10" (25.4 cm), H 2.5" (6.5 cm)
- Baudot Code 45.5
- 1 Start Sit, 5 Databits, 1 Stop Bit
- 120V AC Adapter with 9V custom 1700 mAh battery

OPTIONAL:

- TTY Bag
- Dust Cover
- Cell Phone Connector

Krown Manufacturing, Inc.
3408 Indale Road
Fort Worth, TX 76116
Voice: (817) 738-2485
TTY: (817) 738-8993
Fax: (817) 738-1970
E-mail: info@KrownMfg.com
Website: www.KrownMfg.com

NOTE: Krown products carry a 1-Year Limited Warranty



For use with analog phone lines.

CapTel® 840

See captions of everything your caller says!

Be sure of what people say over the phone with the new CapTel 840. This remarkable phone works like any traditional telephone, but it also shows you written captions during your telephone conversations. Can't quite hear what they say? Just check the captions!

Requires

- Analog telephone line(s). If you have DSL service, a DSL filter is needed. Not compatible with PBX systems unless analog port available. Not designed for use with digital cable, VOIP or cellular telephone services. CapTel 840 can receive calls from cell phone users.*
- Standard electrical power (AC adapter plugs into standard wall outlet).

** People who use digital cable or VOIP telephone service should consider the CapTel 840i which supports these telephone services.*

CapTel®
Captioned Telephone

Benefits of CapTel 840

- Extra large, easy-to-read captions window with adjustable font sizes and colors.
- Built-in Answering Machine shows you captions of your voice messages.
- Display screen tilts for comfortable reading or lies flat to mount the phone on a wall.
- Adjustable volume control (up to 40dB gain) for captioned calls. Volume button is easy to see and adjust during a call.
- One-touch access to CapTel Customer Service (speed dial button automatically connects you to CapTel help line). Available 24 hours a day/7 days a week.
- Easy-to-follow menu system with Yes/No questions.
- Phone Book allows you to store and dial more than 95 names/phone numbers.
- Speed dial keys for one-touch dialing of frequently called numbers.
- Caller-ID capable – shows you who is calling directly on display screen (requires Caller-ID service).
- Spanish-to-Spanish captioning available, with Spanish-language menus.

Optional Capabilities

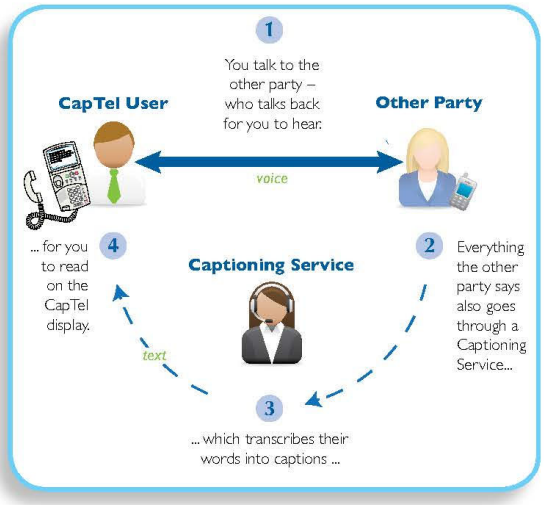
* **2-Line Mode Option:** Lets callers dial your telephone number directly instead of calling through the Captioning Service. This optional method of using CapTel requires a second telephone line (Line 2 must be analog or DSL with filter).

With CapTel Model 840

Captions are provided by a free service that connects to the call.

- Calls you make are automatically connected to the Captioning Service to provide captions.
- People who call you dial the service first, then enter your phone number in order for you to get captions.*
- Works just like a standard phone for people who do not need captions. Just turn captions feature off!
- Compatible with most headsets and assistive listening devices.
- Easy access to your voice mail and answering machine messages.

How CapTel 840 Works:



For more CapTel options visit **www.CapTel.com**

Specifications subject to change.

CapTel is the latest innovation from

Ultratec.

CapTel is a registered trademark of Ultratec, Inc.

1-800-233-9130
Weitbrecht Communications, Inc.
1500 Olympic Blvd Santa Monica CA 90404
(310) 656-4924
(310)450-9918 (Fax)
www.Weitbrecht.com
CapTel@Weitbrecht.com

Distributed by

WCI

903-518900 08/12

sPhone XL

The sPhone XL terminal is a correctional-facility grade, tamper-proof steel enclosure. The hardware is wall mounted unit equipped with a built-in shatter resistant touch screen, a high-resolution video camera with integrated lighting, and tamper-proof, heavy molded plastic handset with an armor-reinforced cord for audio communication, and surge protection.

The terminal includes the following:

- A detention grade hardened steel enclosure
- One detention grade audio handset per terminal for the inmate, and two detention grade audio handsets per terminal for the public
- A shatter resistant LCD monitor with integrated camera
- Enclosures which prevent spills from entering
- Terminals that do not have any openings exposed to the user, including all wiring and ventilation holes
- Terminals without any external hinges
- Terminals are powered by 110 VAC, low voltage DC, or IEEE802.3at (PoE Plus).
- Rounded tops and corners
- Terminals with built-in LED lighting that automatically activates during video visitation sessions and automatically ends when the video visitation session completes and/or disables during all other functions
- Terminals that use standards based videoconferencing CODEC
- Terminals with multiple mounting methods: wall, table, pedestal or cart. All mounting options use standard industry or better methods
- Options for powering the units on and off

Technical Specifications

- Light and ruggedized vandal-proof terminals (hardened steel): Best balance between weight and resistance
- Sealed: Dust and Liquids Resistant, spill-proof (accidental or deliberate).
- Assembly elements are hidden: No screws or hinges can be removed and used to manufacture weapons. No doors/compartments that can be opened in the front or on the sides of the unit.
- Rounded edges that reduce the risks of accidental or intentional injuries.

- Abrasion and chemical resistant; the unit can be cleaned using commercial cleaning agents.
- Humidity and corrosion resistant
- Built-in LCD 15” with hardened shatter resistant touch screen
- HD camera, autofocus, (720p @ 30 fps)
- Sphone XL PoE has movable camera with a 2MP (1600x1200) resolution
- Optional hands free terminal with built-in HD video camera, Pan-Tilt-Zoom, 10x optical zoom, 4x digital zoom, 30fps
- Built-in LED lighting system
- Power ON LED indicator
- Magnetically activated pushbutton for on/off power
- Built-in heat sink mounted to the back for heat dissipation
- Built-in protection device against voltage variations
- Vandal-proof handset. Armored cable
- Standard non-proprietary computer components
- All electrical components comply with UL, CE and/ or CSA
- System maintenance via wireless keyboard (Infra Red Access)
- Mother board: Micro/Mini ATX
- Intel Quad Core 2 GHz processor
- Memory: DDR3; RAM 4,096 MB (4 GB)
- Solid State (SSD) Hard drives to reducing moving components and potential failure points.
- Network: Ethernet RJ-45 (CAT5/6)
- Power Options:
    - AC: 110V 2 amps
    - Low voltage DC: 24 V 8.33 amps
    - Power over Ethernet: IEEE802.3at (PoE Plus).

Terminal Type	Height	Width	Depth	Weight
sPhone XL Single Handset	20.5	20	6	43
sPhone XL Dual Handset	20.5	23	6	44.6
sPhone XL Hands Free	23	17.375	6	49
sPhone XL Hands Free w/ PTZ camera	29.75	17.375	6	54.8
sPhone XL Single Handset PoE	20.5	20	4.25	38.6

sPhone XL Dual Handset PoE	20.5	23	4.25	40.2

- Manufactured according to ISO 9001:2008
- FCC Part 15 class A compliant
- sPhone XL PoE is CE compliant
- Touch Screen is UL-60950 and CSA 22.2 No. 60950 ball drop test compliant
- Touchscreen meets IEC: 60529
- Touchscreen meets IP: 544
- Touchscreen meets NEMA: Type 12
- AC power Supply Meets Electrical Standard: CSA: 22.2
- MTBF: 80,000 hours approx.

XL2

At the core of incarcerant services is the new XL^2 Incarcerant Kiosk. Incarcerants use this kiosk to access digital content (music, movies, games, educational materials, and news), compose (or upload) and send email, send eCards, attend video visitation sessions, log into their JPay account, and send grievances to facility staff. It can also support any Securus-based services available via the current sPhone XL terminal and its ConnectUs application suite, which means that a single kiosk installation can handle all of the DOC's offender communications needs.

The kiosk incorporates a standard size keyboard, trackball mouse, and wrist rest space. It accommodates numerous mounting options, such as wall, tabletop, cart, and pedestal.

Kiosk Specifications

- Hardened steel enclosure with anti-vandal security lock and bolts
- Built-in LED Lighting
- Dimensions: 22¾ "x 21" x 4¼ "
- Weight: 50 lbs. (including PC & networking components)
- High strength scratch-resistant security glass
- Dynamic handset with secured caps and a 32" armored cord
- stainless steel keyboard with trackball and braille keys
- Power - Power over Ethernet, 802.3at (PoE+), 25 watts
- MTBF: 80,000 hours

Encased Components

- 17” LCD hardened touchscreen monitor with integrated privacy screen
- Screen resolution 1280x1024
- 5 megapixel autofocus camera with 2592x1944 max resolution
- Quad core processor
- 4 GB RAM
- 512 GB mSATA hard drive
- Armored USB cable
- Cat6 Ethernet Port

The keyboard and trackball are resistant to liquid, dust, and debris. The keyboard is integrated into a sealed metal base so that its components are spill-proof. The kiosk is also designed so that spilled liquids flow away from important componentry if they do somehow reach the inside of the kiosk. All electrical components are compliant with UL, CE, and/or CSA standards.

Parts can only be removed from a kiosk by a technician. Kiosks are vandal-proof and are treated well because they provide a valuable service to the incarcerant population.

Kiosks have smooth stainless steel surfaces with no sharp edges. If cleaning is necessary, kiosks are easily wiped down since all exterior parts are water-resistant, including the keyboard and handset.

Securus technicians can quickly open the enclosure and swap components. Components are designed and fastened so that the technician can quickly detect a problem and replace a particular component, most of them, or all of them if necessary.

JP6 Tablet Hardware

Inmate Tablet Designation:

SECURUS JP6

Features:

- Ruggedized Casing
- High strength, impact-resistant security glass w/ integrated screen protector
- Barrel charge port
- Pogo pin connector
- Secure Wi-Fi
- Built-in FM Radio Receiver

Specs:

- Internal Storage: 32 GB
- CPU: MT8163 - Quad core cortex A9 Frequency 1.3G, 64bit CPU
- Resolution: 1280 x 800
- Dimensions: (L x W x H) 7.8” x 5” x 0.61”
- Weight: 17.2 Oz
- Battery: Lithium - 500 cycles, includes temperature sensor
- Dual Wi-Fi Bands (2.4GHz and 5GHz)

Environmental Conditions:

- Operating Temperature Range: *50º F to 110º F (10º C to 43º C)*
- Storage Temperature Range: *-40º F to 150º F (-40º C to 65º C)*
- Humidity: *95% RH (relative humidity), non-condensing*

Item	JP5S	JP6S
OS	Android 5.1	Android 8.1
CPU	CPU RK3188 - Quad core cortex A53, Frequency 1.3G, 64bit CPU	MT8163 - Quad core cortex A9, Frequency 1.6G, 32bit CPU
GPU (Graphics Processing Unit)	Mali-400MP4	Mali-T720 MP2 GPU
DDR	1G – 512*8	2G - 512*8
BATTERY	4000mAh	8000mAh
LCD	Resolution: 1024*600	Resolution: 800*1280
Boot On - mA during boot on	460 mA	500-750 mA (LCD on)
Stand by: Stand by current on main window	560 mA (LCD on)	300-400 mA (LCD on)
Music: Listen to music w/ ear bud plug in	580 mA (LCD on)	380-400 mA (LCD on)
Movie: Play movie w/ ear bud plugged in	650 mA (LCD on)	450-550 mA (LCD on)
FM: Listen to FM w/ ear bud plugged in	600 mA (LCD on)	300-400 mA (LCD on)
Back Light	545 mA	380 mA
USB (OTG)	700 mA	400 mA
Stand by time	About 7hrs with LCD on About 250hrs with LCD off	About 22hrs with LCD on About 350hrs with LCD off
Play MP3	About 6.5hrs with LCD on About 47hrs with LCD off	About 20hrs with LCD on About 140hrs with LCD off
Play Video	About 5hrs	About 13-14hrs
Storage	32GB	32GB
Buttons	Power, volume up, volume down	Power, volume up, volume down
5G	N/A	Dual support for 2.4G and 5G
CAMERA	N/A	2 Mega Pixel
POGO PIN	N/A	YES – charging and mounting

ADTRAN

Data Sheet

NetVanta

3140

Fixed Port Secure Access Ethernet Router

Gigabit | eSBC Ready | VQM

Benefits

- 100 Mbps router with three Gigabit Ethernet interfaces
- Provides capability for Ethernet redundancy
- USB interface for integrated 3G/4G backup
- Voice Quality Monitoring (VQM) and Mean Opinion Score (MOS) prediction
- Utilizes standards-based routing protocols utilized by the widely deployed NetVanta Series
- Compatible with industry leading softswitches and call agents
- Dynamic bandwidth allocation affords more efficient utilization
- Stateful inspection firewall for network security
- Quality of Service (QoS) for delay and jitter sensitive traffic like VoIP
- Supports 802.1q Virtual LAN (VLAN) Trunking
- Optional IPSec Virtual Private Network (VPN) for secure corporate connectivity across the Internet
- Command Line Interface (CLI) mimics industry de facto standard
- Network Address Translation (NAT) for IP address concealment
- Wi-Fi® Access Controller for centralized management of NetVanta Wireless Access Points (WAPs)
- Feature-rich ADTRAN® Operating System (AOS)
- Available in desktop or rack mountable versions
- Industry-leading, North American five-year warranty
- Optional full featured eSBC for robust network security and voice interoperability

Overview

The NetVanta® 3140 is a fixed-port, high-performance Ethernet router supporting converged access and high-quality voice services. It provides three routed, autosensing Gigabit Ethernet interfaces. This product is ideal for carrier-bundled service offerings, and enterprise class Internet access for secure, high-speed corporate connectivity. The NetVanta 3140 is available as either a desktop, or rack mountable platform.

Flexibility and Redundancy

The NetVanta 3140 is ideal for multiple applications where Ethernet redundancy is needed given the three Gigabit ports that can be either LAN or WAN facing. This can be achieved with two Ethernet delivered access services providing immediate failover to the active link anytime a link down event occurs. In addition, the NetVanta 3140 features USB interface that can be used for 3G/4G backup.

Many deployments still feature separate voice and data networks, and the NetVanta 3140 is a perfect fit for these as well with a single WAN link, the other two Gigabit interfaces can accomplish this.

Standards Protocols

The versatile hardware platform of the NetVanta 3140 is further complemented with the AOS. The AOS allows for the support of static and default routes, demand and policy based routing, and allows for fast, accurate network convergence using routing protocols such as BGP, OSPF, RIP, and PIM Sparse Mode for multicast routing. Multihoming is also available to provide redundant or backup WAN links to multiple ISPs, guaranteeing a wide-area connection.

Hierarchal QoS

QoS is also supported for delay-sensitive traffic like VoIP or video. To prioritize mission-critical traffic and control network congestion, the NetVanta 3140 uses Low Latency Queuing, Weighted Fair Queuing (WFQ), Class-based WFQ, and DiffServ marking to establish the priority of IP packets routed over the WAN.

VoIP Ready

In combination with the QoS features, a specialized SIP ALG allows SIP traffic to traverse NAT-enabled firewalls. For enterprise networks, this interoperability allows IP PBXs, phones, and other SIP-based devices to set up, tear down, and pass voice and call control messages seamlessly through the integral NAT-enabled firewall.

The NetVanta 3140 also deploys VQM to capture MOS, jitter, delay, and packet loss statistics necessary to troubleshoot VoIP calls over the WAN. This powerful, yet graphically intuitive, diagnostic tool allows for quick isolation of network issues to ensure superior call quality.

NETVANTA 3140

Enterprise Session Border Control (eSBC)

The NetVanta 3140 can provide optional eSBC functionality delivering a truly converged application platform at the customer premises. This feature is becoming mandatory in today's service deployment to normalize, secure and troubleshoot the SIP to SIP communication between a carrier network and the customers SIP compliant equipment.

Security

The AOS provides a powerful, high-performance stateful inspection firewall. The firewall can identify and protect against common Denial of Service (DoS) attacks like TCP syn flooding, IP spoofing, ICMP redirect, ping-of-death, and IP reassembly problems.

In addition, the AOS is capable of providing an inherent URL-filtering package without the use of an external server. URL filtering is another level of security that allows system administrators to restrict Internet access by permitting or denying specific URLs. This URLfiltering feature also includes the ability to produce top website reports of the most frequently requested websites, allowing system administrators to modify the URL filter lists.

The NetVanta 3140 also adds the support for IPSec compliant VPN. The NetVanta 3140 supports encryption algorithms like DES, 3DES, and AES. With this upgrade, the NetVanta 3140 is fully compatible with other IPSec VPN equipped NetVanta products.

Management

The NetVanta 3140 Series can be remotely managed by ADTRAN's n-Command® MSP platform. ADTRAN n-Command platforms offer the ability to discover devices, make mass configuration changes or firmware upgrades, backup/restore configuration, and generate inventory reports for asset management. The ADTRAN n-Command MSP also offers VoIP VQM and reporting, as well as an industry-leading, easy-to-use, Graphical User Interface (GUI). NetVanta 3140 is available in rack mountable, and desktop versions; and are backed by an industry-leading warranty.

Administration

The AOS offers an intuitive Web-based GUI that provides step-by-step configuration wizards, management capability, and the ability to upload firmware updates. In addition, it has a standard CLI that mimics the widely adopted, industry de facto standard. The sequence of commands required to configure similar devices is almost identical, eliminating training costs typically associated with learning a new operating system or obtaining costly industry certifications. The CLI also allows for configuration scripts to be used, saved, and downloaded as a quick-and-easy recovery mechanism.

Product Specifications

Physical Interfaces

- Ethernet
- Full Duplex
- Auto-negotiation
- RJ-45
- USB 2.0
- One Port
- Console Port
- Three Gigabit Ethernet Interfaces (WAN/LAN Support)
- Supports 802.1q VLAN Trunking
- EIA-232 Providing Local Management and Configuration (via a DB-9 Female Connector)

Diagnostic LEDs

- Stat (Power)
- Gig 1, Gig 2, Gig 3 (Ethernet)
- USB

Protocols

- EBGP/IBGP
- RIP (v1 and V2)
- PIM Sparse Mode
- IGMP V2
- GRE
- PPP Dial Backup
- PAP and CHAP
- Multi-VRF CE
- VRRP
- Policy-based Routing
- OSPF
- PPPoE
- Multilink PPPoE
- Demand Routing
- RFC 1483
- Multihoming
- Layer 3 Backup
- TWAMP

Quality of Service (QoS)
- Low Latency and Weighted Fair Queuing (WFQ)
- Class-Based WFQ
- DiffServ Packet Marking and Recognition
- Traffic Monitoring (NetFlow 9)

Voice Quality Monitoring (VQM)
- Mean Opinion Score (MOS) Prediction
- Jitter, Delay and Packet Loss
- Past and Active Calls

Traffic and Network Quality Monitoring
- ICMP and TWAMP Probes and Tracks
- One-Way Delay
- Round-Trip Loss and Delay
- Inter-Packet Delay Variance
- Traffic Flow Collection and Analysis
- Packet Capture

Administration
- Familiar Command Line Interface (CLI)
- Web-Based GU
- n-Command Support
- SNMP V2 and V3
- SYSLOG Logging
- Email Alerts (SMTP)
- Policy Statistics
- TCL Scripting
- Login Privilege Levels
- Telnet, Craft/Console Port, SSH, Ping, Trace Route and NTP

DHCP
- Client, Server and Relay

Firewall
- Stateful Inspection Firewall
- Denial of Service (DOS) Protection
- Access Control Lists
- Application Level Gateways
- Packet Filtering

Network Address Translation
- Basic NAT (1:1), NAPT (Many:1) and 1:1 Port Translation
- NAT-compatible SIP ALG

NAT Traversal and Remote Survivability
- B2BUA
- SIP Registrar for IP Phones
- SIP Proxy with Survivability
- Transparent/Stateful/Outbound

Content Filtering
- Inherent URL Filtering
- Top Website Reports
- Integration with Websense

Secure Management
- Multi-level Access Control
- TACACS+
- RADIUS AAA
- SSH CLI and SSL GUI
- Port Authentication (802.1x)

VPN (Optional)
- **IPSec Tunnel Mode:** 500 Tunnels
- **Encryption:** DES, 3DES and AES
- **Authentication Mechanisms:** XAUTH, Digital Certificates, Pre-shared Keys and Secure ID

Environment
- **Operating Temperature:** 32° to 122° F (0° to 50° C)
- **Storage Temperature:** -40° to 158° F (-20° to 70° C)
- **Relative Humidity:** Up to 95%, Non-condensing

Physical and Power
NetVanta 3140
- Self Standing, Desktop Plastic Enclosure
- **Dimensions:** 1.63 in. x 9 in. x 6.38 in. (H x W x D), (4.14 cm x 22.86 cm x 16.21 cm)
- **Weight:** 1 lbs. (.45 kg)
- **Power:** DC (12 VDC, 1.0 A)

NetVanta 3140 RM
- 1U Metal Rackmount
- **Dimensions:** 1.72 in. x 8.4 in. x 8 in. (H x W x D), (4.36 cm x 21.3 cm x 20.3 cm)
- **Weight:** 3 lbs. (1.4 kg)
- **Power:** AC (Auto-ranging, 100 to 250 VAC, 50/60 Hz, 0.4 A Maximum)

Agency Approvals
- FCC Part 15 Class A
- CE Mark
- UL & Canadian UL
- RoHS
- C-Tick for Australia and New Zealand

Ordering Options

Hardware Options	Part No.
Multi-Service Edge Switch	
NetVanta 3140 Desktop	1700340F1
NetVanta 3140	1700341F1
NetVanta 3140 Desktop with VPN and VQM	4700340F2
NetVanta 3140 with VPN and VQM	4700341F2
VPN and VQM Software Upgrade	1950340F2
19 in. Rackmount Brackets*	1700511F1
19 in. Dual Mounting Tray*	1700508F1
Wall Mount*	1200884G1
Dual Wall Mount*	1700512F1
NetVanta 3140 with SBC, 5 Calls	4700341F2#5
NetVanta 3140 with SBC, 10 Calls	4700341F2#10
NetVanta 3140 with SBC, 25 Calls	4700341F2#25
NetVanta 3140 with SBC, 50 Calls	4700341F2#50
NetVanta 3140 with SBC, 100 Calls	4700341F2#100
NetVanta 3140 with SBC, 300 Calls	4700341F2#300
Software Options	
NetVanta 3140 SBC Upgrade, 5 Calls	1963SBCF5
NetVanta 3140 SBC Upgrade, 10 Calls	1963SBCF10
NetVanta 3140 SBC Upgrade, 25 Calls	1963SBCF25
NetVanta 3140 SBC Upgrade, 50 Calls	1963SBCF50
NetVanta 3140 SBC Upgrade, 100 Calls	1963SBCF100
NetVanta 3140 SBC Upgrade, 300 Calls	1963SBCF300

* Accessories apply to NetVanta 3140 (non-desktop version) only

ADTRAN, Inc.
901 Explorer Boulevard
Huntsville, AL 35806
256 963-8000

General Information
800 9ADTRAN
www.adtran.com/contactus

Canada Headquarters—Toronto, Ontario
+1 877 923 8726
+1 905 625 2515
sales.canada@adtran.com

Canada—Montreal, Quebec
+1 877 923 8726
+1 514 940 2888
sales.canada@adtran.com

Mexico and Central America
+1 256 963 3321
+1 52 55 5280 0265 Mexico
sales.cala@adtran.com

South America
+1 256 963 3185
sales.brazil@adtran.com
sales.latam@adtran.com

61700340F1-8E

NetVanta 1534

Layer 3 Lite Gigabit Ethernet Switch

Product Features

- 28-port multi-layer Gigabit Ethernet switch
- 24-Gigabit Ethernet ports and four SFP optical ports
- Two standard 1 Gbps SFP ports and two enhanced 2.5 Gbps SFP ports
- Non-blocking, up to 62 Gbps switching capacity
- Line rate Layer 2 and Layer 3 Lite capabilities
- 16 static routes
- 802.1Q VLANs, Private VLANs and VLAN assignment via 802.1x
- VoIP Setup Wizard
- Advanced QoS with support for 802.1p and DiffServ prioritization with four queues per egress port
- Automate actions with Port Scheduler and TCL scripting
- VoIP ready with LLDP/LLDP-MED and voice VLANS
- Business-class security with RADIUS, TACACS+, 802.1x and port security
- Optimized for iSCSI Storage Area Networks (SANs) solutions
- Wi-Fi® access controller for centralized management of NetVanta Wireless Access Points (WAPs)
- Cable and SFP diagnostics provides easy to use trouble-shooting tools for copper and fiber cable
- Familiar CLI and Web GUI
- Limited lifetime warranty
- Next business day advance replacement

NetVanta® 1534 is a managed, 28-port, Layer 3 Lite, Gigabit Ethernet switch designed as an access layer or network backbone switch for Small to Medium-sized Enterprises (SMEs). With the combination of the advanced multi-layer switching fabric, high-bandwidth capabilities, and enhanced Quality of Service (QoS) features, the NetVanta 1534 is ideal in Gigabit-to-the-desktop deployments, and converged voice and data networks.

Hardware

The NetVanta 1534 rackmountable switch provides 28 Gigabit Ethernet ports, consisting of 24 fixed 10/100/1000Base-T Ethernet ports, two 1.0 Gbps Small Form-factor Pluggable (SFP) ports, and two 2.5 Gbps enhanced SFP ports located on the back. Together the four SFP ports can provide up to 14 Gbps of bandwidth between interconnected NetVanta 1534 switches. "Halfrack" in size, you can scale to 48 Gigabit Ethernet ports and eight SFP optical ports utilizing two NetVanta 1543 switches side-by-side in a single 19-inch rack space.

Multi-layer Switching

The NetVanta 1534 supports advanced multi-layer (Layer 2 and Layer 3 Lite) switching with up to 16 static routes allowing it to easily scale from SMBs to enterprise-size networks.

VoIP Ready

The NetVanta 1534 is VoIP-ready with the ability to automatically configure IP phones using LLDP-MED, and the ability to separate voice traffic onto voice VLANs, to simplify the deployment of VoIP. In addition, the switch includes a VoIP Setup Wizard (available via a Web-based Graphical User Interface (GUI) or Command Line Interface (CLI)), which automates the complete VoIP setup process reducing deployment time and eliminating errors. An on-demand VoIP report provides a printable summary of the switch VoIP configuration, as well as providing alerts and recommendations to improve performance. All NetVanta switches support QoS to prioritize VoIP traffic, 802.1p and DiffServ Class of Service (CoS).

Security

The NetVanta 1534 offers a variety of data security features including DoS protection, MAC-based port security, multilevel user passwords, Secure Shell (SSH) and Secure Socket Layer (SSL) for encrypted user login, and Access Authentication and Authorization (AAA) for authentication with RADIUS and TACACS+. With features such as 802.1x and port security, administrators can assure that only authorized users are allowed access to the network.

The ADTRAN® Operating System (AOS) also features desktop auditing using DHCP in conjunction with Microsoft Network Access Protection (NAP) protocol to monitor the health of client computers. The two protocols work together to ensure that systems connected to the network are using appropriate corporate policies, such as firewall settings, antivirus settings and other client health information.

Port Scheduler

NetVanta 1534 allows ports to be enable or disabled based on time of day. This ability to schedule available ports allows for added security and can provide less power consumption during off hours saving on utility cost.

iSCSI Optimized

All ADTRAN NetVanta Gigabit Ethernet switches are optimized for iSCSI SANs deployments. Network administrators can take advantage of features such as Jumbo frame support (up to 13K), separation of iSCSI network traffic utilizing VLANs, and 802.3x flow control to seamlessly integrate ADTRAN switches with iSCSI SANs devices.

Administration

AOS offers both a CLI and an intuitive Web-based GUI with step-by-step configuration wizards. For automating setup and configuration, NetVanta 1534 supports Auto-Config which provides the ability to automatically obtain the switch configuration via DHCP.

AOS also offers network forensics to aid in troubleshooting network problems by allowing network administrators to easily locate devices on the network by MAC or IP address.

ADTRAN, Inc.
Attn: Enterprise Networks
901 Explorer Boulevard
Huntsville, AL 35806
P.O. Box 140000
Huntsville, AL 35814-4000

256 963-8000
256 963-8699 fax

General Information
800 9ADTRAN
info@adtran.com
www.adtran.com

Pre-Sales Technical Support
888 423-8726
application.engineer@adtran.com
www.adtran.com/presales

Post-Sales Technical Support
888 423-8726
support@adtran.com
www.adtran.com/support

Where to Buy
888 423-8726
channel.sales@adtran.com
www.adtran.com/where2buy

ProServices℠
888 874-2237
proservices@adtran.com
www.adtran.com/proservices

Global Inquiries
256 963-8000
256 963-6300 fax
international@adtran.com

ADTRAN is an ISO 9001, ISO 14001, and a TL 9000 certified supplier.

6170259OG1-8E July

NetVanta 1534

Layer 3 Lite Gigabit Ethernet Switch

Product Specifications

Physcial Interface

Ethernet Ports

- 24 –10/100/1000Base-T
- 2–Standard 1 Gbps SFP ports
- 2–Enhanced 1.0/2.5 Gbps SFP Ports
- Auto rate/duplex/MDI/MDI-X

Console Port

- DB-9, RS-232

Switching Performance

- Non-blocking Layer 2/3 Switching

Maximum Forwarding Bandwidth

- 62 Gbps

Layer 2 Support

- 802.1D Spanning Tree
- 802.1w Rapid STP
- 802.3ad Link Aggregation
- 8,000 MAC Addresses
- Jumbo Frames (9K)
- IGMP Snooping
- 802.3x Flow Control

Layer 3 Support

- 16 Static Routes
- 8 Layer 3 Interfaces
- UDP Relay
- 232 ARP Entries
- IPv6 Management

Diagnostics

- Port Mirroring
- LLDP (802.1AB)
- LLDP-MED
- Cable Diagnostics
- SFP Diagnostics
- Troubleshooting Page

Front Panel Status LEDs

- Power Status
- **LAN:** link, activity

Port Statistics

- Number of TX/RX Frames, Collisions, Errors

Quality of Service

- 802.1p and DiffServ
- Four output queues per egress port
- Weighted Round Robin (WRR)
- Strict Priority Scheduling

VLAN

- Port-based VLANs
- 802.1Q tagged trunked VLANs
- Voice VLANs
- Private VLAN Edge
- Dynamic 802.1x assigned VLANs
- Support for up to 255 active VLANs

Storm Control

- Broadcast, Unicast, and Multicast

Administration

- CLI (Console/Telnet/SSH)
- SNMP v3
- Web-based GUI (HTTP/SSL)
- SYSLOG
- n-Command® support
- Email Alerts
- RADIUS
- TACACS+
- TCL Scripting
- Auto Config
- Port Scheduler
- DHCP Network Forensics

Security

- Port authentication (802.1x)
- Port Security
- DoS Protection
- Hardware ACLs
- Microsoft Desktop Auditing

Wi-Fi Controller

- Controls up to 24 NetVanta WAPs

Environment

- **Operating Temperature:** 32° to 122° F (0° to 50° C)
- **Storage Temperature:** -4° to 158° F (-20° to 70° C)
- **Relative Humidity:** Up to 95%, non-condensing

Physical

- **Chassis:** 1U, 19 in. Rackmountable Metal Enclosure (Rackmount Brackets Included)
- **Dimensions:** 1.72 in. x 8 in. x 11 in. (4.4 cm x 20.3 cm x 27.9 cm) (H x W x D)
- **Weight:** 4 lbs. (2.72 kg.)
- **AC Power:** 100–250 VAC, 50/60 Hz
- **Power:** 30 Watts, 1 A Max

Agency Approvals

- FCC Part 15 Class A, UL 1950/CSA, CE Mark, C-tick, RoHS

Ordering Information

Equipment	Part No.
NetVanta 1534	**1702590G1**
NetVanta 1000BaseSX SFP Transceiver	**1200480E1**
NetVanta 1000BaseLX SFP Transceiver	**1200481E1**
NetVanta 2.5 Gbps Multimode SFP Transceiver	**1200482G1**
NetVanta 2.5 Gbps Singlemode SFP Transceiver	**1200483G1**
NetVanta 1 Meter SFP Interconnect Cable	**1200484G1**
NetVanta 3 Meter SFP Interconnect Cable	**1200484G3**
Dual Mounting Tray	**1700508F1**
Wall Mount Brackets	**1700507F1**

NetVanta 1534P

Layer 3 Lite Gigabit Ethernet Switch

Product Features

- 28-port multi-layer Gigabit Ethernet switch
- 24-Gigabit Ethernet ports and four SFP optical ports
- Two standard 1 Gbps SFP ports and two enhanced 2.5 Gbps SFP ports
- 802.3af (PoE), 802.3at (PoE+) and Legacy PoE
- Non-blocking, up to 62 Gbps switching capacity
- Line rate Layer 2 and Layer 3 Lite capabilities
- DHCP network forensics
- 802.1Q VLANs, Private VLANs and VLAN assignment via 802.1x
- VoIP Setup Wizard
- Advanced QoS with support for 802.1p and DiffServ prioritization with four queues per egress port
- Automate actions with Port Scheduler and TCL scripting
- VoIP ready with LLDP/LLDP-MED and voice VLANS
- Business-class security with RADIUS, TACACS+, 802.1x and port security
- Optimized for iSCSI Storage Area Networks (SANs) solutions
- Wi-Fi® access controller for centralized management of NetVanta Wireless Access Points (WAPs)
- Cable and SFP diagnostics provides easy to use trouble-shooting tools for copper and fiber cable
- Familiar CLI and Web GUI
- Limited lifetime warranty
- Next business day advance replacement

The NetVanta® 1534P is a managed, 28-port PoE, Layer 3 Lite, Gigabit Ethernet switch designed for fast, secure, cost-effective Local Area Network (LAN) switching. This scalable, full-featured business-class switch is perfect for higher-bandwidth Voice over IP (VoIP) applications needing PoE to power IP Phones, as well as Gigabit-to-the-desktop deployments. Experience the ease of management with an easy-to-use Web-based Graphical User Interface (GUI) and familiar Command Line Interface (CLI).

Hardware

The NetVanta 1534P rackmount switch provides 28 Gigabit Ethernet ports, consisting of 24 fixed 10/100/1000Base-T Ethernet ports, two 1.0 Gbps Small Form-factor Pluggable (SFP) ports, and two 2.5 Gbps enhanced SFP ports. Together the four SFP ports can provide up to 14 Gbps of bandwidth between interconnected NetVanta 1534P switches.

Multi-layer Switching

The NetVanta 1534P supports advanced multi-layer (Layer 2 and Layer 3 Lite) switching with up to 16 static routes allowing it to easily scale from SMBs to enterprise-size networks.

VoIP Ready

The NetVanta 1534P is VoIP-ready with the ability to automatically configure IP phones using LLDP-MED, and the ability to separate voice traffic onto voice VLANs, to simplify the deployment of VoIP. In addition, the switch includes a VoIP Setup Wizard (available via a Web-based Graphical User Interface (GUI) or Command Line Interface (CLI)), which automates the complete VoIP setup process reducing deployment time and eliminating errors. An on-demand VoIP report provides a printable summary of the switch VoIP configuration, as well as providing alerts and recommendations to improve performance. All NetVanta switches support QoS to prioritize VoIP traffic, 802.1p and DiffServ Class of Service (CoS).

PoE

The NetVanta 1534P provides up to 370 watts of 802.3af (PoE), 802.3at (PoE+) and Legacy PoE for powering IP phones, wireless access points (WAPs), and other devices requiring LAN power.

Supplemental PoE Power

When deployed with the NetVanta 1131 RPS/EPS unit, the NetVanta 1534P supports power redundancy as well as enhanced PoE. The NetVanta 1131's EPS output provides up to 370 watts of backup PoE for redundancy, and can also provide up to 370 watts of additional PoE, effectively doubling the available PoE budget (up to 740 watts).

Security

The NetVanta 1534P offers a variety of data security features including DoS protection, MAC-based port security, multilevel user passwords, Secure Shell (SSH) and Secure Socket Layer (SSL) for encrypted user login, and Access Authentication and Authorization (AAA) for authentication with RADIUS and TACACS+. With features such as 802.1x and port security, administrators can assure that only authorized users are allowed access to the network.

The ADTRAN® Operating System (AOS) also features desktop auditing using DHCP in conjunction with Microsoft Network Access Protection (NAP) protocol to monitor the health of client computers. The two protocols work together to ensure that systems connected to the network are using appropriate corporate policies, such as firewall settings, antivirus settings and other client health information.

Port Scheduler

NetVanta 1534P allows ports to be enable or disabled based on time of day. This ability to schedule available ports allows for added security and can provide less power consumption during off hours saving on utility cost.

iSCSI Optimized

All ADTRAN NetVanta Gigabit Ethernet switches are optimized for iSCSI SANs deployments. Network administrators can take advantage of features such as Jumbo frame support (up to 13K), separation of iSCSI network traffic utilizing VLANs, and 802.3x flow control to seamlessly integrate ADTRAN switches with iSCSI SANs devices.

Administration

AOS offers both a CLI and an intuitive Web-based GUI with step-by-step configuration wizards. For automating setup and configuration, NetVanta 1534P supports Auto-Config which provides the ability to automatically obtain the switch configuration via DHCP.

AOS also offers network forensics to aid in troubleshooting network problems by allowing network administrators to easily locate devices on the network by MAC or IP address.

ADTRAN, Inc.
Attn: Enterprise Networks
901 Explorer Boulevard
Huntsville, AL 35806
P.O. Box 140000
Huntsville, AL 35814-4000

256 963-8000
256 963-8699 fax

General Information
800 9ADTRAN
info@adtran.com
www.adtran.com

Pre-Sales Technical Support
888 423-8726
application.engineer@adtran.com
www.adtran.com/presales

Post-Sales Technical Support
888 423-8726
support@adtran.com
www.adtran.com/support

Where to Buy
888 423-8726
channel.sales@adtran.com
www.adtran.com/where2buy

ProServices℠
888 874-2237
proservices@adtran.com
www.adtran.com/proservices

Global Inquiries
256 963-8000
256 963-6300 fax
international@adtran.com

ADTRAN is an ISO 9001, ISO 14001, and a TL 9000 certified supplier.

61702591G2-8A September

NetVanta 1534P

Layer 3 Lite Gigabit Ethernet Switch

Product Specifications

Physcial Interface

Ethernet Ports

- 24 –10/100/1000Base-T
- 2–Standard 1 Gbps SFP ports
- 2–Enhanced 1.0/2.5 Gbps SFP Ports
- Auto rate/duplex/MDI/MDI-X

Console Port

- DB-9, RS-232

Switching Performance

- Non-blocking Layer 2/3 Switching

Maximum Forwarding Bandwidth

- 62 Gbps

Layer 2 Support

- 802.1D Spanning Tree
- 802.1w Rapid STP
- 802.3ad Link Aggregation
- 8,000 MAC Addresses
- Jumbo Frames (13K)
- IGMP Snooping
- 802.3x Flow Control

Layer 3 Support

- 16 Static Routes
- 8 Layer 3 Interfaces
- UDP Relay
- 232 ARP Entries
- IPv6 Management

Diagnostics

- Port Mirroring
- LLDP (802.1AB)
- LLDP-MED
- Cable Diagnostics
- SFP Diagnostics
- Troubleshooting Page

Front Panel Status LEDs

- Power Status
- **LAN:** link, activity

Port Statistics

- Number of TX/RX Frames, Collisions, Errors

Quality of Service

- 802.1p and DiffServ
- Four output queues per egress port
- Weighted Round Robin (WRR)
- Strict Priority Scheduling

VLAN

- Port-based VLANs
- 802.1Q tagged trunked VLANs
- Voice VLANs
- Private VLAN Edge
- Dynamic 802.1x assigned VLANs
- Support for up to 255 active VLANs

Storm Control

- Broadcast, Unicast, and Multicast

PoE

- 802.3af (PoE) and 802.3at (PoE+) and Legacy PoE
- 370 Watts (Total)
- Extended PoE Budget up to 740W (when connected to the NetVanta 1131)

Administration

- CLI (Console/Telnet/SSH)
- SNMP v3
- Web-based GUI (HTTP/SSL)
- SYSLOG
- n-Command® support
- Email Alerts
- RADIUS
- TACACS+
- TCL Scripting
- Auto Config
- Port Scheduler
- DHCP Network Forensics

Security

- Port authentication (802.1x)
- Port Security
- DoS Protection
- Hardware ACLs
- Microsoft Desktop Auditing

Wi-Fi Controller

- Controls up to 24 NetVanta WAPs

Environment

- **Operating Temperature:** 32° to 122° F (0° to 45° C)
- **Storage Temperature:** -4° to 158° F (-20° to 70° C)
- **Relative Humidity:** Up to 95%, non-condensing

Physical

- **Chassis:** 1U, 19 in. Rackmountable Metal Enclosure (Rackmount Brackets Included)
- **Dimensions:** 1.72 in. x 17.2 in. x 10 in. (4.4 cm x 43.7 cm x 25.4 cm) (H x W x D)
- **Weight:** 9.5 lbs. (4.3 kg.)
- **AC Power:** 110–230 VAC, 50/60 Hz
- **Power:** 500 Watts, 4.9 A Max

Agency Approvals

- FCC Part 15 Class A, UL 1950/CSA, RoHS

Ordering Information

Equipment	Part No.
NetVanta 1534P	**1702591G2**
NetVanta 1000BaseSX SFP Transceiver	**1200480E1**
NetVanta 1000BaseLX SFP Transceiver	**1200481E1**
NetVanta 2.5 Gbps Multimode SFP Transceiver	**1200482G1**
NetVanta 2.5 Gbps Singlemode SFP Transceiver	**1200483G1**
NetVanta 1 Meter SFP Interconnect Cable	**1200484G1**
NetVanta 3 Meter SFP Interconnect Cable	**1200484G3**
NetVanta 1131 (RPS/EPS)	**1700530F1**
NetVanta 1131 RPS Cable	**1700532F1**
NetVanta 1131 EPS Cable	**1700533F1**

ZoneFlex R600

Dual-Band 802.11ac 3X3:3 Smart Wi-Fi Access Points

Ruckus
Simply Better Wireless.

DATA SHEET

BENEFITS

EXTENDED RANGE REQUIRES FEWER APS

Adaptive antenna technology delivers up to 2x increase in Wi-Fi signal coverage minimizing the number of APs required to service any area

SLEEK, LOW PROFILE ENCLOSURE FOR EASE-OF-DEPLOYMENT

Aesthetically-pleasing design and a range of mounting options

CHANNEL SELECTION OPTIMIZES THROUGHPUT

ChannelFly dynamic channel management, based on throughput measurements, not just interference, chooses the best channel to give users the highest possible throughput

SUPER SIMPLE CONFIGURATION AND MANAGEMENT

The industry's simplest configuration and management through a Web-based wizard

FLEXIBLE DEPLOYMENT OPTIONS

Standalone or controller-based migration

ADAPTIVE POLARIZATION DIVERSITY (PD-MRC)

Dual-polarized antennas that are dynamically selected provide better reception for hard to hear clients and more consistent performance as clients constantly change orientation

HASSLE FREE MIGRATION TO HIGHER SPEED WI-FI

Support for standard 802.3af power over Ethernet allows enterprises to use existing PoE switches without costly upgrades

802.11AC HIGH PERFORMANCE MID-RANGE 3X3:3 SMART WI-FI ACCESS POINTS WITH ADAPTIVE ANTENNA TECHNOLOGY

The Ruckus ZoneFlex R600 delivers high-performance and reliable 802.11ac wireless networking at a competitive price point for medium density venues such as in K-12 or Higher ED..

The ZoneFlex R600 combines patented adaptive antenna technology and automatic interference mitigation to deliver consistent, predictable performance at extended ranges with up to an additional 6dB of BeamFlex gain on top of the physical antenna gain and up to 15dB of interference mitigation.

The R600 is ideal for wireless networks servicing mobile devices with dual-polarized antennas that adapt in real time to maximize performance for the mobile enterprise.

Performance is further enhanced as the ZoneFlex R600 integrates Ruckus' patented BeamFlex, a software-controlled, high gain adaptive antenna technology. The ZoneFlex R600 automatically selects channels for highest throughput potential using Ruckus ChannelFly dynamic channel management, adapting to environmental changes.

A sleek and low-profile design, the ZoneFlex R600 was purpose-built for small-medium enterprises requiring reliable high speed client connectivity. It is ideal for a variety of medium density enterprise and hotspot environments including SMB's such as independent hotels, local retailers and non-franchise restaurants.

ZoneFlex R600

Dual-Band 802.11ac 3X3:3 Smart Wi-Fi Access Points

DATA SHEET

PATENTED BEAMFLEX™ TECHNOLOGY EXTENDS SIGNAL RANGE, IMPROVES STABILITY OF CLIENT CONNECTIONS

All ZoneFlex R600 Wi-Fi access points integrate a software-controlled smart antenna with PD-MRC (polarization diversity) that delivers up to an additional 6dB of BeamFlex gain and 15dB of interference mitigation. This is especially beneficial to enhance the performance of mobile devices which are constantly in motion and changing orientation.

ADVANCED WLAN APPLICATIONS

Each ZoneFlex R600 supports a wide range of value-added applications such as guest networking, Dynamic PSK, hotspot authentication, wireless intrusion detection and many more. In a controller-less configuration, the ZoneFlex R600 works with a wide range of authentication servers including Microsoft's Active Directory, and AAA/RADIUS.

FLEXIBLE DEPLOYMENT OPTIONS

Ruckus is custom-designed to help small business owners grow their business, deliver an excellent customer experience and manage costs while supporting Wi-Fi and a variety of mobile devices with minimal IT staff.

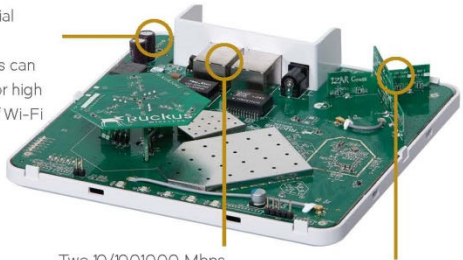
COMPLETE LOCAL AND REMOTE MANAGEMENT

Each ZoneFlex R600 can be managed as a standalone AP through a Web-based GUI, using SNMP or through the Ruckus SCI or FlexMaster. Local management can also be performed using Ruckus' Smart WLAN controllers. FlexMaster is a LINUX-based software platform that uses industry standard protocols to perform bulk configuration, fault detection, monitoring and a wide range of trouble-shooting capabilities over a wire area connection. The controllers enable local management and control of APs, adding value-added services such as transmit power control and guest networking.

FEATURES

- Dual-band concurrent (2.4GHz/5GHz)
- Adaptive antenna technology and advanced RF management
- Up to an additional 6dB BeamFlex gain / 15dB interference mitigation / 3dBi physical antenna gain
- Automatic interference mitigation, optimized for high-density environments
- Integrated smart antenna technology
- Standard 802.3af Power over Ethernet (PoE)
- DHCP services
- IP multicast video streaming support
- Advanced QoS packet classification and automatic priority for latency-sensitive traffic
- Dynamic, per user rate-limiting for hotspot WLANs
- WPA-PSK (AES), 802.1X support for RADIUS and Active Directory
- BYOD, Zero-IT and Dynamic PSK
- Admission control/load balancing
- Band steering and airtime fairness support
- Rich and customizable guest access services
- Application recognition and control
- Bonjour gateway
- SecureHotspot
- Band balancing
- SmartMesh
- SPoT location services

Many potential antenna combinations can be chosen for high availability of Wi-Fi



Two 10/1001000 Mbps ports; one with PoE

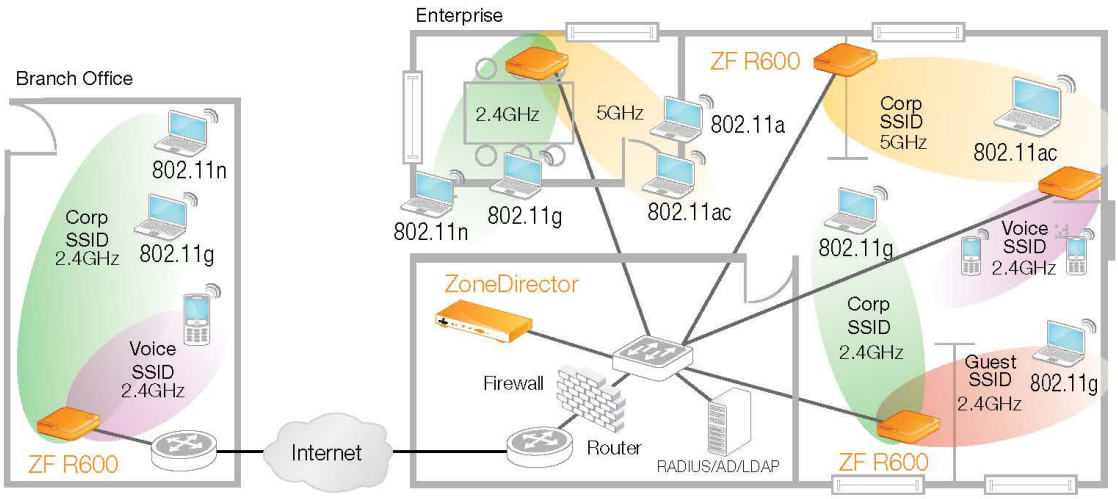
High-gain directional antenna elements not only delivers signal gain but also interference mitigation for range extension, reliability and high data rates

ZoneFlex R600

Dual-Band 802.11ac 3X3:3 Smart Wi-Fi Access Points

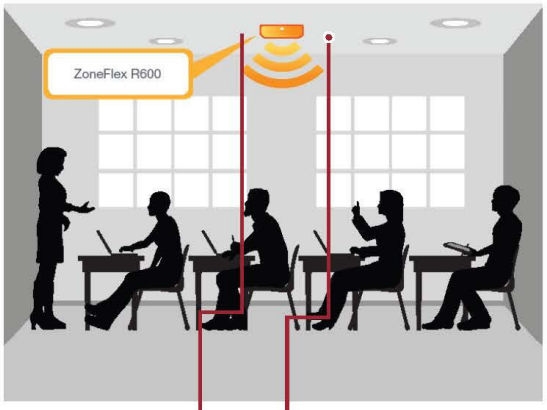
DATA SHEET

The ZoneFlex R600 integrates with your existing network infrastructure, delivering best-in-class 802.11ac performance and reliability at a competitive price -- making it the ideal wireless solution for mid-range enterprise and branch office applications.



DEPLOYMENTS FOR CLASSROOMS AND LIBRARIES

The ZoneFlex R600 is ideal for deployment in education common areas providing high quality wireless access in high density locations

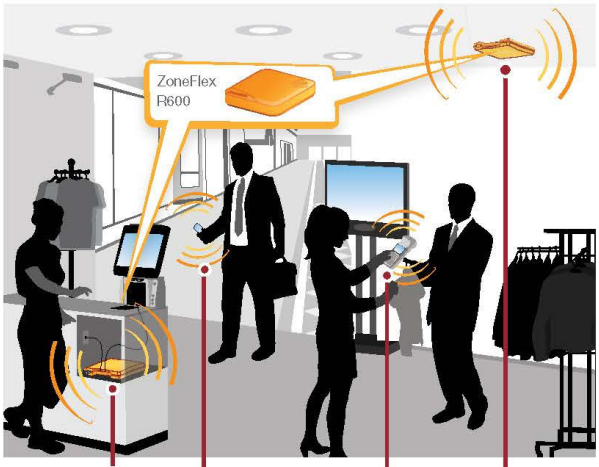


Dual-band (2.4/5GHz) support allows for concurrent Internet and IP-based video services

Sleek, elegant design easily concealed

DEPLOYMENT FOR RETAIL/BRANCH OFFICES

The ZoneFlex R600 is ideal for deployment in retail stores to provide inconspicuous wireless connection tohigh quality video, wireless IP phones and data accessfor handheld PoS barcode scanners



Wired ports to connect devices such as cash registers, printers, etc.

Multiple SSIDs for differentiated user services (e.g., guest Wi-Fi, point of sale, voice)

Reliable Wi-Fi connectivity for point of sale devices

5GHz band and smart antenna system ideal for 802.11ac clients

ZoneFlex R600

Dual-Band 802.11ac 3X3:3 Smart Wi-Fi Access Points

DATA SHEET

PHYSICAL CHARACTERISTICS	
Power	• DC Input 12 VDC 1.0A • Power over Ethernet 802.3 af
Physical Size	• 15.8 cm x 15.8 cm x 4 cm (6.2 in x 6.2 in x 1.57 in)
Weight	• 364 g (0.8 lb.)
Data Ports	• 2 auto MDX, auto-sensing 10/100/1000 Mbps, RJ-45, POE port (on one port)
Lock Options	• Hidden latching mechanism • Kensington Lock Hole • T-bar Torx • Bracket (902-0108-0000) Torx screw & padlock (sold separately)
Environmental Conditions	• Operating Temperature: 0°C – 40°C • Operating Humidity: 10% – 95% non-condensing
Power Draw	• Idle: 4W • Typical: 6.2W • Peak: 11.2W

PERFORMANCE AND CAPACITY	
Concurrent Stations	• Up to 512 clients per AP
Simultaneous Voip Clients	• Up to 30 clients per AP

RF	
ANTENNA	• Adaptive antenna that provides up to 512 unique antenna patterns per radio • Full omnidirectional polarization diversity
PHYSICAL ANTENNA GAIN	• Up to 3dBi
BEAMFLEX* SINR TX GAIN	• Up to 6dB
BEAMFLEX* SINR RX GAIN	• 3-5dB (PD-MRC)
INTERFERENCE MITIGATION	• Up to 15dB
MINIMUM RX SENSITIVITY	• Up to -101dBm

* BeamFlex gains are statistical system level effects translated to enhanced SINR based on observations over time in real-world conditions with multiple APs and many clients

MANAGEMENT	
Deployment Options	• Standalone (individually managed) • Managed by ZoneDirector (9.8.1 & Above) • Managed by SmartZone (3.0 & above) • Managed by FlexMaster • Managed by SmartCell™ Gateway 200 (2.5 & above)
Configuration	• Web User Interface (HTTP/S) • CLI (Telnet/SSH), SNMP v1, 2, 3 • TR-069 vis FlexMaster
Auto Ap Software Updates	• FTP or TFTP, remote auto available

WI-FI	
Standards	• IEEE 802.11a/b/g/n/ac • 2.4GHz and 5GHz
Supported Data Rates	• 802.11n/ac: 6.5Mbps – 260Mbps (20MHz) • 13.5Mbps – 600Mbps (40MHz) • 29.3Mbps – 1.300Mbps (80MHz) • 802.11a: 54, 48, 36, 24, 18, 12, 9 and 6Mbps • 802.11b: 11, 5.5, 2 and 1 Mbps • 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6Mbps
Radio Chains	• 3 x 3
Spatial Streams	• 3
RF POWER OUTPUT (Aggregate)	• 28 dBm for 2.4GHz† • 27 dBm for 5GHz†
Channelization	• 20MHz, 40MHz, 80MHz
Operating Channels	• US/Canada: 1-11, Europe (ETSI X30): 1-13, Japan X41: 1-13 • 5 GHz channels: Country dependent
Frequency Band	• IEEE 802.11 b/g/n: 2.4 – 2.484GHz • IEEE 802.11a/ac: 5.15 – 5.25GHz; 5.25 – 5.35GHz; 5.47 – 5.725 GHz; 5.725 – 5.85GHz
Power Save	• Supported
Wireless Security	• WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i • Authentication via 802.1X with the ZoneDirector, local authentication database, support of RADIUS, and ActiveDirectory
Certifications**	• US, Europe, Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Costa Rica, Egypt, Hong Kong, India, Indonesia, Israel, Japan, Korea, Malaysia, Mauritius, Mexico, New Zealand, Pakistan, Peru, Philippines, Russia, Saudi Arabia, Singapore, South Africa, Taiwan, Thailand & UAE. • WEEE/RoHS compliance • EN-60601-1-2 (Medical) • Wi-Fi Alliance • EN50121-1 Railway EMC • EN50121-4 Railway Immunity • IEC 61373 Railway Shock & Vibration • UL 2043 plenum rated • 5GHz UNII-1 (2014)

† Maximum power varies by country
** For current certification status please see price list

PRODUCT ORDERING INFORMATION

MODEL	DESCRIPTION
ZoneFlex R600 Smart Wi-Fi 802.11ac Access Point	
901-R600-XX00	Concurrent dual band 802.11ac Access Point, no power adapter
Optional Accessories	
902-0108-0000	• Spare, Accessory Mounting Bracket
902-0173-XXYY	• Power Adapter, AC/DC wall plug,100-240Vac 50/60Hz
902-0162-XXYY	• PoE injector (sold in quantities of 10 or 100)

PLEASE NOTE: When ordering ZoneFlex Indoor APs, you must specify the destination region by indicating -US, -WW, or -Z2 instead of XX. When ordering PoE injectors or power supplies, you must specify the destination region by indicating -US, -EU, -AU, -BR, -CN, -IN, -JP, -KR, -SA, -UK, or -UN instead of -XX.

For access points, -Z2 applies to the following countries: Algeria, Egypt, Israel, Morocco, Tunisia, and Vietnam

Warranty: Sold with a limited lifetime warranty.
For details see: http://support.ruckuswireless.com/warranty

Ruckus Wireless, Inc. | 350 West Java Drive | Sunnyvale, CA 94089 USA | T: (650) 265-4200 | F: (408) 738-2065
ruckuswireless.com

The Eaton 3S — Sleek. Savvy. Sophisticated.

The sleek, new Eaton® 3S delivers high efficiency and energy-saving battery backup and surge protection for your premium home and office equipment — ready to go right out of the box.

Eaton 3S features and benefits:

Ease-of-use: The plug-and-play functionality of the 3S allows you to start backing up your equipment the moment you take the unit out of the box. Gain automatic integration with Windows, Mac and Linux with a simple connection to a USB port.

EcoControl: The 3S manages your energy efficiency for you with EcoControl Master/Control outlets. When the item using the Master outlet (e.g., your computer) is idle or shut down, then items using the Control outlets (e.g., printer, scanner, fax) are automatically powered down – rewarding you with up to 30% in energy savings over a typical battery backup.

Modern design: The sleek design of the 3S allows you to display it alongside your high-tech equipment for a sophisticated look. This unit can also be wall- or desk-mounted for additional space savings.

Premium protection: The high-efficiency design of the Eaton 3S provides premium power protection for up to 10 devices, including those using data lines.

Intelligent Power Protector

By combining Eaton's Intelligent Power® Protector software with the 3S, you can monitor and manage all of the power devices on your network. You can even enable graceful shutdown of computers during an extended power outage.

To learn more, please visit:
www.eaton.com/intelligentpower

Services and support

Eaton provides product support 24 hours a day, 7 days a week. From battery replacement to full service plans, Eaton is one of the top service models in the industry.

Three-year warranty

The 3S warranty covers both the UPS and the batteries for three years. No other manufacturer in the industry offers as comprehensive a warranty.

Battery runtime

The 3S provides up to 45 minutes of battery backup. For a detailed interactive battery runtime chart, please visit **www.eaton.com/3S** — then view the individual technical specifications pages for details of each unit.

EATON
Powering Business Worldwide

The compact, versatile 3S fits under a desk or mounts on the wall.

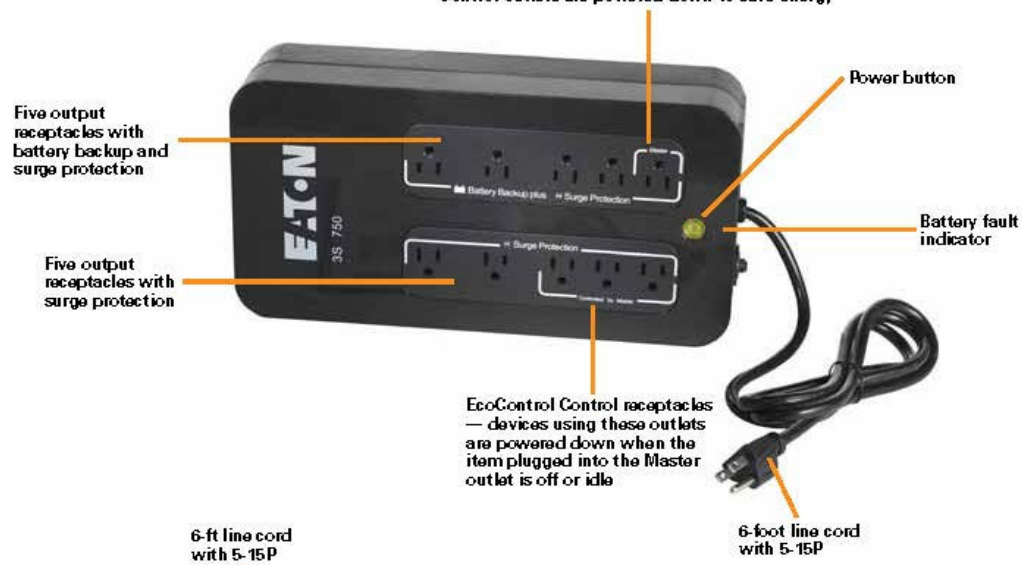
Celebrating 100 YEARS
Ideals that Endure

3S MODEL SELECTION GUIDE*

Catalog Number	Power rating (VA/Watts)	Input connection	Output receptacles***	Dimensions (H x W x D), in	Net weight, lb
120V, 50/60 Hz					
3S550	550/330	5-15P	(8) 5-15R	3.4 x 5.5 x 13.2	7.3
3S750**	750/450	5-15P	(10) 5-15R	3.4 x 6.7 x 13.2	9.7

* Due to continuous product improvement programs, all specifications are subject to change without notice. Please visit www.eaton.com/3S to view complete product specifications.
** This model has EcoControl energy savings capability. To enable EcoControl, download Eaton's Personal Solution Pac software: www.eaton.com/psp.
*** On each unit, half of the receptacles provide battery backup and surge protection, half provide surge protection only.

Eaton 3S (750 VA)



To interact with the 3S, please visit:
eaton.com/3S

Eaton Corporation
8609 Six Forks Road
Raleigh, NC 27615
United States
800.356.5794

Eaton.com/powerquality

The 3S is part of the UPSgrade program

UPSgrade™
www.eaton.com/UPSgrade

Tripp Lite
1111 W. 35th Street
Chicago, IL 60609 USA
Telephone: 773.869.1234
www.tripplite.com

DataShield In-Line Surge Protector for Network and Phone Lines, 1-Line RJ45

MODEL NUMBER: **DNET1**

Protects network datalines on workstations, printers, hubs and other devices from blown NIC cards, garbled transmissions, lock-ups and hardware failures caused by surges, line noise, ESD, faulty wiring and lightning.

Description

Tripp Lite's DNET1 provides network Ethernet line surge suppression for 100Base-T, 10Base-T, Token Ring, AS400/Sys3x and RS422 applications. Surge suppression is handled with balanced arrays of high-speed avalanche diodes that divert excess energies created by electrostatic discharges, faulty wiring or lightning away from network interface connections. Tripp Lite network surge suppressors reduce blown NIC cards, garbled network transmissions, system lock-ups and hard equipment failure by safely shunting dataline surges to ground. Convenient RJ45 input and output connections with an included 5-inch Ethernet patch cable enables ideal protection for network workstations, printers and other internetworking devices with a network connection. For peace of mind, the DNET1 comes with a lifetime warranty and RoHS-compliant design.

Features

- DNET1 protects network workstations, printers and internetworking devices from surges present on 10/100Base-T, token ring, AS400/Sys3x or RS422 network lines
- Convenient RJ45 input and output connections make for simple installation (RJ45 input/output connections, pins 1-8, 7.5V clamping)
- 5 inch Ethernet patch cable enables ideal protection placed as close as possible to the point of use
- Surge suppression utilizing high speed avalanche diodes divert excess energies on the network to ground
- RoHS Compliance
- Lifetime Warranty

Highlights

- Network Ethernet line surge suppression for 100Base-T, 10Base-T, Token Ring, AS400/Sys3x and RS422 applications
- Ideal protection for NICs, terminals, hubs, printers, LAN equipment, and other internetworking devices
- Protects against the effects of electrostatic discharge, faulty wiring and lightning
- Reduces blown NIC cards, garbled network transmissions, system lock-ups and hard equipment failure
- 750A circuit breaker; 7.5V nominal clamping voltage
- RJ45 input and output connections with included patch cable

Package Includes

- DNET1 dataline protector
- 5-in. RJ45 patch cable
- Warranty information and instruction manual

Specifications

OVERVIEW	
UPC Code	037332011435
OUTPUT	
Output Receptacles	(1) Network
Circuit Breaker (amps)	750
Right-Angle Outlets	No
INPUT	
Nominal Input Voltage(s) Supported	120V AC; 230V AC
Recommended Electrical Service	120V, 230V
Input Plug Type	RJ45
Input Cord Length (ft.)	0
Right-Angle Plug	No
Input Cord Length (m)	0.00
Integrated Cord Clip	No
USER INTERFACE, ALERTS & CONTROLS	
Diagnostic LED(s)	No
SURGE / NOISE SUPPRESSION	
AC Suppression Joule Rating	0
Clamping Voltage (RMS)	7.5
Auto Shut-Off	No
DATALINE SURGE SUPPRESSION	
Telephone/DSL Protection	Yes
Telephone/DSL Protection Details	1 line
Cable (Coax) Protection	No
Network (Ethernet) Protection	Yes
Additional Dataline Protection	1-8
PHYSICAL	
Anti-Microbial Protected	No
Color	Light Gray

Tripp Lite
1111 W. 35th Street
Chicago, IL 60609 USA
Telephone: 773.869.1234
www.tripplite.com

Integrated Keyhole Mounting Slots	No
Shipping Dimensions (hwd / cm)	15.24 x 7.62 x 5.08
Shipping Dimensions (hwd / in.)	6.00 x 3.00 x 2.00
Shipping Weight (kg)	0.11
Shipping Weight (lbs.)	0.23
WARRANTY	
Product Warranty Period (Worldwide)	Lifetime limited warranty

SurgeGate
Enduring Surge Protection

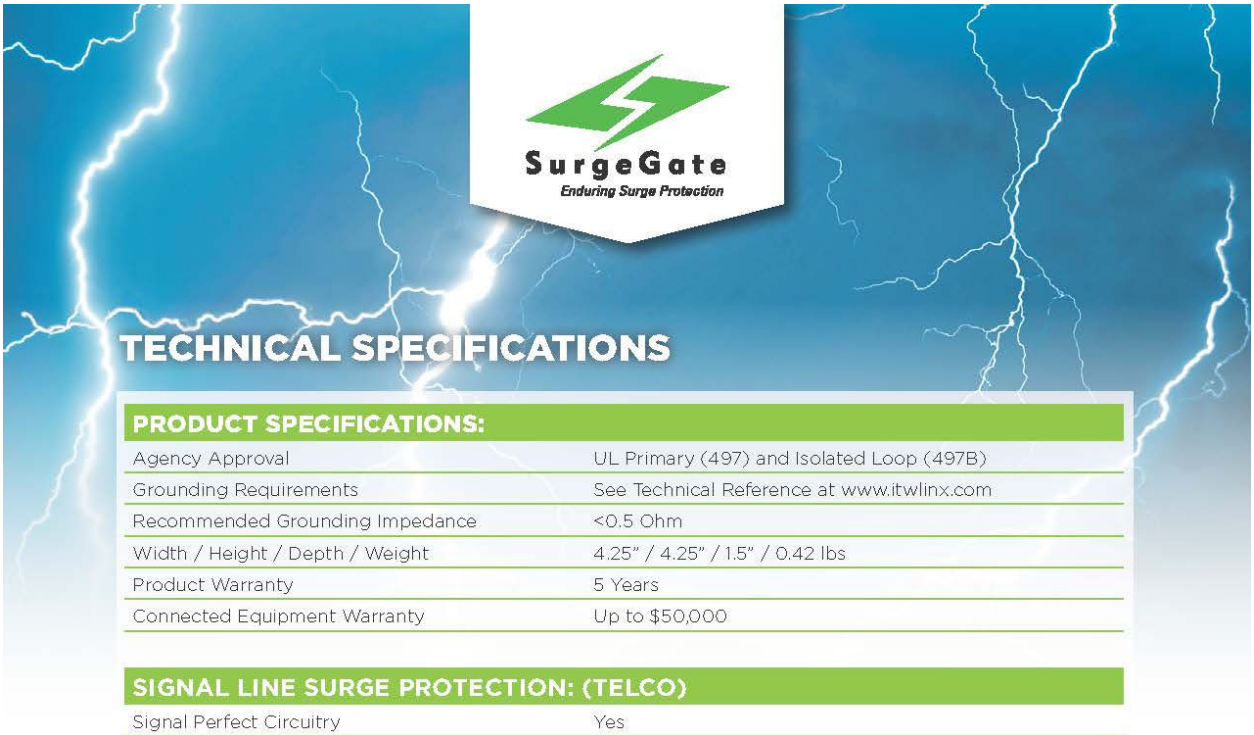
CAT6-75-110 IN/RJ 45 OUT - SOLID-STATE BUILDING ENTRANCE PROTECTORS

Features:

- UL listed for Primary (497) and Isolated Loop (497B) applications
- Exceeds TIA/EIA Standards 568 and 758 for CAT6 performance
- Solid-state protection for fastest response
- Use between buildings in a campus environment as a building entrance protector or in hostile industrial applications as an isolated loop protector
- For use with **CISCO** POE systems
- Can be used in high power POE (POE+) applications
- **Expandable System Protection** - SurgeGate Modules can be attached to one another to expand system protection as your system grows
- **5 Year Product Warranty** - This surge protector shall be free of any defects in design, materials, or workmanship, or ITW Linx will repair or replace the defective product
- **$50,000 Connected Equipment**

ITW Linx®
Surge Protection Solutions

Questions on ordering? Call us at 1-800-278-5666
Visit us at: www.itwlinx.com



TECHNICAL SPECIFICATIONS

PRODUCT SPECIFICATIONS:	
Agency Approval	UL Primary (497) and Isolated Loop (497B)
Grounding Requirements	See Technical Reference at www.itwlinx.com
Recommended Grounding Impedance	<0.5 Ohm
Width / Height / Depth / Weight	4.25" / 4.25" / 1.5" / 0.42 lbs
Product Warranty	5 Years
Connected Equipment Warranty	Up to $50,000

SIGNAL LINE SURGE PROTECTION: (TELCO)	
Signal Perfect Circuitry	Yes
Fused	Yes
Performance Rating	Cat6
Clamping Level	75V
Response Time	1-5 Nanoseconds
Capacitance	<5pF
Wires Protected	4-pairs
Termination Type	110 Punchdown In/RJ 45 Out

ORDERING INFORMATION

Part Number	Description
CAT6-75-110 In/RJ 45 Out	Protects high-performance 4-pair CAT6 Outside Plant Cables as well as CAT6 UTP cables for voice or ISDN low-voltage (digital, 75V) applications. Uses 110 punchdown In/RJ45 Out.

ITW Linx®
Surge Protection Solutions

Questions about ordering? Please contact us at 1-800-336-5469
Contact an authorized distributor for pricing
Visit us at www.itwlinx.com

Compact, flexible desktops designed to provide all the essentials your business needs.

OptiPlex 3050 Tower, Small Form Factor and Micro

More power

Intel® 7th generation processors allow for the fastest OptiPlex yet with support up to Core™ i5

Stay flexible

Versatile suite of stand and mounting options to tailor your workspace to max out on productivity

Service with ease

Entry tool-less design and simple removeable side panel to service and expand effortlessly

Stay secure

With TPM, chassis intrusion switch, Dell Data Protection and cable covers for certain form factors, you can work more and focus less on security risks

Features & Technical Specifications

Feature	3050 Tower/Small Form Factor/Micro Technical Specifications
Processor[1]	Intel ® 7th generation Celeron, Pentium and Core™ i3 Dual Core, Core™ i5 Quad Core (up to 65W Tower/Small Form Factor, 35W Micro); supports Win 10/Linux Intel ® 6th generation Celeron, Pentium and Core™ i3 Dual Core, Core™ i5 Quad Core (up to 65W Tower/Small Form Factor, 35W Micro); supports Win 7/8.1/10/Linux
Chipset	Intel® B250 Chipset
Operating System[1]	Microsoft® Windows 7 Pro (32/64-bit) with Windows 10 Pro License (requires Intel® 6th generation processors) Microsoft® Windows 7 Embedded (OEM only) Microsoft® Windows 10 Home (64-bit) Microsoft® Windows 10 Pro (64-bit) Microsoft® Windows 10 Embedded (OEM only) Ubuntu® 16.04 LTS (64-bit) Neokylin® v6.0 (China only)
Graphics Options[2]	Integrated Intel® HD Graphics 610/630 (with Intel® 7th generation processors) Integrated Intel® HD Graphics 510/530 (with Intel® 6th generation processors) Supports optional discrete graphics Tower/Small Form Factor: 1GB/2GB AMD Radeon™ R5 430, 4GB AMD Radeon™ R7 450
Memory[2,3]	2 DIMM slots (2 SODIMM slots for Micro); Non-ECC dual-channel 2400MHz DDR4 SDRAM. (Memory performance on Intel® 6th generation processors will be at 2133MHz). Max memory 32GB
Networking	Integrated Realtek® RTL8111H Ethernet LAN 10/100/1000 Optional wireless: Intel® 8265 802.11ac+ Bluetooth 4.2[13] card; Intel ® 3165 802.11ac+ Bluetooth 4.2[14] card
I/O Ports	**Tower/Small Form Factor:** 8 External USB: 4 x USB 3.1 Gen 1 (2 front/2 rear) and 4 x USB 2.0 (2 front/2 rear); 2 Internal USB 2.0; 1 RJ-45; 1 Display Port 1.2; 1 HDMI 1.4; 1 UAJ, 1 Line-out; 1 VGA (optional); Serial+PS/2 (optional) **Micro:** 6 External USB: 4 x USB 3.1 Gen 1 (2 front/2 rear) and 2 x USB 2.0 (2 rear); 1 RJ-45; 1 HDMI 1.4; 1 Display Port 1.2; 1 UAJ (front); 1 Line-out (front); additional DisplayPort 1.2 (optional); 1 VGA (optional); Serial+PS2 (optional); Serial (optional)
Security Options	Trusted Platform Module[6] TPM 1.2 or 2.0, Dell Data Protection| Encryption, Microsoft Windows Bitlocker, Local HDD data wipe via BIOS ("Secure Erase"), Encryption - SED HDD (Opal FIPS), Chassis lock slot support, Lockable Port Cover, Chassis Intrusion Switch, D-Pedigree (Secure Supply Chain Functionality), Setup/BIOS Password, Optional Smart Card keyboards, Intel® Trusted Execution Technology, Intel® Identity Protection Technology, Dell Secure Works, firmware support for optional Absolute Data & Device Security (formerly Computrace)[7], Intel Software Guard eXtensions

Storage[4] **Options (internal)**	Hard disk drives: up to 2 TB; solid state drives: up to 512 GB. Dual storage support Supports Hybrid, Opal SED FIPS, M.2 PCIe Solid State Drive Intel® Optane™ Memory Ready	**Environmental, Ergonomic, & Regulatory Standards**	Environmental Standards (eco-labels): ENERGY STAR 6.1 qualified, EPEAT Registered[9], TCO Certified, CEL, WEEE, Japan Energy Law, South Korea E-standby, South Korea Eco-label, EU RoHS, China RoHS[14]. Please see your local representative or www.dell.com for specific details
Removable Media Options	Supports optional optical disc drives and media card reader (Tower/ Small Form Factor only)	**Configuration Services**	Factory Image load. BIOS Customization. Hardware Customization, asset tagging and reporting
Systems Management Options[8]	Dell Client Command Suite for in-band systems management	**Warranty**	Limited Hardware Warranty[10]; Standard Next Business Day On Site Service after Remote Diagnosis[11]; Optional Dell ProSupport offers premium support from expert technicians and 24x7 availability[12]

Chassis		Tower	Small Form Factor	Micro
	Dimensions (H x W x D)(inches/cm)	13.8 x 6.1 x 10.8 / 35 x 15.4 x 27.4	11.4 x 3.7 x 11.5 / 29 x 9.7 x 29.2	7.2 x 1.4 x 7.0 18.2 x 3.6 x 17.8
	Min. Weight (lbs/kg)	17.49 / 7.93	11.42 / 5.14	2.6 / 1.18
	Number of Bays	1 internal 3.5" HDD 2 internal 2.5" HDD/SSD 1 external slim ODD	1 x 3.5" HDD or 2.5" HDD/SDD 1 external slim ODD	1 internal 2.5" bay
	Expansion Slots	1 full height PCIe x16 3 full height PCIe x1 1 M.2 (22x80mm / 22x42mm)	1 half height PCIe x16 1 half height PCIe x1 1 M.2 (22x80mm / 22x42mm)	1 M.2 (22x30mm) 1 M.2 (22x80mm / 22x42mm)
	Power Supply[1,5] Unit (PSU)	Standard 240W PSU Active PFC 240W typical 85% Efficient PSU (80 PLUS Bronze) ENERGY STAR compliant, Active PFC 240W typical 92% Efficient PSU (80 PLUS Platinum); ENERGY STAR compliant, Active PFC	Standard 180W PSU Active PFC 180W typical 85% Efficient PSU (80 PLUS Bronze) ENERGY STAR compliant, Active PFC 180W typical 92% Efficient PSU (80 PLUS Platinum); ENERGY STAR compliant, Active PFC	65W external adapter with 87% minimum average efficiency for use with 35W processors

Essential Accessories

OptiPlex 3050 Tower, Small Form Factor and Micro

At The Desk

Dell OptiPlex Small Form Factor All-in-One Stand

Dell OptiPlex Micro All-in-One Stand

Dell OptiPlex Micro DVD+/-RW Drive Enclosure

Dell OptiPlex Micro VESA Mount

Dell OptiPlex Micro All in One Mount for E-Series Displays

Dell Pro Stereo Headset UC350

Dell OptiPlex Tower or Small Form Factor Cable Cover

Dell Wireless Keyboard and Mouse KM636

Dell 24 Monitor P2417H (dual set up)

Compact, flexible desktops designed to provide all the essentials your business needs.

OptiPlex 3050 Tower, Small Form Factor and Micro

Discover professional class desktops at www.dell.com/OptiPlex

1. Offering and availability may vary by region. Some items available after product introduction. For complete details, refer to the Technical Guidebook published on www.dell.com.
2. System Memory and Graphics: Significant system memory may be used to support graphics, depending on system memory size and other factors.
3. 4GB or Greater System Memory Capability: A 64-bit operating system is required to support 4GB or more of system memory.
4. Storage: GB means 1 billion bytes and TB equals 1 trillion bytes; actual capacity varies with preloaded material and operating environment and will be less.
5. PSU: This form factor utilizes a more efficient Active Power Factor Correction (APFC) power supply. Dell recommends only Universal Power Supplies (UPS) based on Sine Wave output for APFC PSUs, not an approximation of a Sine Wave, Square Wave, or quasi-Square Wave (see UPS technical specifications). If you have questions please contact the manufacturer to confirm the output type.
6. TPM: Not available in all regions.
7. Absolute Data & Device Security (formerly Computrace): Not a Dell offer. Certain conditions apply. For full details, see terms and conditions at www.lojackforlaptops.com.
8. In-Band Systems Management - This option entirely removes Intel out of band systems (OOB) management features. The system can still support in band management. OOB management support through AMT cannot be upgraded post-purchase.
9. Please refer to www.epeat.net for specific country registration rating and participation.
10. Limited Hardware Warranty: For copy of Ltd Hardware Warranty, write Dell USA LP, Attn: Warranties, One Dell Way, Round Rock, TX 78682 or see www.dell.com/warranty.
11. Onsite Service after Remote Diagnosis: Remote Diagnosis is determination by online/phone technician of cause of issue; may involve customer access to inside of system and multiple or extended sessions. If issue is covered by Limited Hardware Warranty (www.dell.com/warranty) and not resolved remotely, technician and/or part will be dispatched, usually within 1 business day following completion of Remote Diagnosis. Availability varies. Other conditions apply.
12. Availability and terms of Dell Services vary by region. For more information, visit www.dell.com/servicedescriptions.
13. Particular versions of Microsoft Windows may not support the full Bluetooth 4.2 functionality
14. For a complete listing of declarations and certifications, refer to the Dell Regulatory and Environmental Datasheet found in the Manuals section of Product Support information http://www.dell.com/support/home/us/en/19

Revised February 2017

Transform how you work.

DELL 22 MONITOR | P2219H

OPTIMIZE YOUR WORKSPACE

Free up valuable desk space with this 21.5" FHD monitor featuring a small footprint and thin panel profile. Easily hide away cable clutter with the improved cable management design.

MAXIMIZE PRODUCTIVITY

The 3-sided ultrathin bezel delivers a seamless view across multiple monitors, while Easy Arrange in Dell Display Manager software helps you stay organized when multitasking.

WORK COMFORTABLY

Pivot, tilt, swivel and adjust the height of your monitor to your exact preference. Stay focused longer with a flicker-free screen and ComfortView that optimize eye comfort.

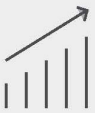
TRUSTED RELIABILITY

Dell monitors — World's number 1 monitor brand[1] Enjoy peace of mind with Dell Premium Panel Exchange, 3 year Advanced Exchange Service[2] and optional ProSupport.[3]

Maximize productivity

OPTIMIZED WORKSPACE

More room to work: Free up valuable desk space with a thin monitor profile and a small monitor base that's approximately 22% smaller than its predecessor.[4]
Clutter-free: Focus on your work while hiding away cable clutter with an improved cable management design.
Consistent and rich colors: A wide viewing angle enabled by In-Plane Switching technology lets you see vibrant colors—no matter where you sit.



MAXIMIZE PRODUCTIVITY

Expand your efficiency: The three-sided ultrathin bezel design lets you enjoy an uninterrupted view of your content across multiple monitors. And, with a Dell dual monitor set up, you can increase your productivity by up to 21%.[5]
More ways to multitask: Work conveniently across multiple screens and select from predefined templates with the Easy Arrange feature on Dell Display Manager software. Quickly tile and arrange your applications and get back to work faster with Auto-restore, a feature that remembers where you left off.

WORK COMFORTABLY

Adjust to your comfort: Pivot, tilt, swivel and adjust the height of your monitor for a comfortable setup all day long. Or choose from a variety of mounts and stands, including VESA, for even more flexibility.
Easy on the eyes: This TÜV[6] Certified monitor has a flicker-free screen with ComfortView, a feature that reduces harmful blue light emissions. It's designed to optimize eye comfort even over extended viewing.

TRUSTED RELIABILITY

DELL MONITORS – WORLD'S NUMBER 1 MONITOR BRAND[1]

Peace of mind: Dell Premium Panel Exchange allows a free panel replacement during the Limited Hardware Warranty[7] period even if only one bright pixel is found.
Minimize downtime: Your monitor comes with a 3-year Advanced Exchange Service[2] so that if a replacement becomes necessary, it will be shipped to you the next business day during your 3-year Limited Hardware Warranty.[7]
Get a higher level of support: Upgrade to 24x7, in-region technical phone support from qualified engineers with Dell ProSupport option.[3]

Features & Technical Specifications

Monitor	Dell 22 Monitor - P2219H
Diagonal Viewing Size	54.61 cm (21.5 inches)
Active Display Area	
Width	476.06 mm (18.74")
Height	267.79 mm (10.54")
Maximum Preset Resolution	1920 x 1080 at 60 Hz
Aspect Ratio	16:9
Pixel Pitch	0.248 mm x 0.248 mm
Pixel Per Inch (PPI)	102
Brightness	250 cd/m² (typical)
Color Support	Color Gamut (typical): 72% (CIE1931)[8] Color Depth: 16.7 Million colors
Contrast Ratio	1000: 1 (typical)
Viewing Angle	178°/178°
Response Time	8 ms (Normal); 5 ms (Fast) - (gray to gray)
Panel Type	In-Plane Switching Technology
Backlight Technology	LED Edgelight System
ComfortView with Flicker-free screen	Yes
Dell Display Manager Compatibility	Yes
Remote Asset Management	Yes, via Dell Command | Monitor
Display Screen Coating	Antiglare with 3H hardness
Connectivity	
Connectors	1 x DisplayPort version 1.2, 1 x HDMI port version 1.4, 1 x VGA port, 1 x USB 3.0 upstream port (bottom), 2 x USB 3.0 downstream ports (side), 2 x USB 2.0 downstream ports (bottom)
Built-in Devices	USB 3.0 super-speed hub (with 1 x USB 3.0 upstream port), 2 x USB 3.0 downstream ports, 2 x USB 2.0 downstream ports
Design Features	
Adjustability	Height-adjustable stand (130 mm), Tilt (-5° to 21°) Swivel (-45° to 45°), Pivot (-90° to 90°)
Security	Security lock slot (cable lock sold separately)
Flat Panel Mount Interface	VESA (100 mm x 100 mm)
Power	
AC input voltage/frequency/current	100 VAC to 240 VAC / 50 Hz or 60 Hz ± 3 Hz / 1.5 A (typical)
Power Consumption (Operational)	17W (typical) / 37W (maximum)[9]
Power Consumption Stand by / Sleep	Less than 0.3W
Dimensions (with stand)	
Height (Compressed ~ Extended)	353.4 mm ~ 472.0 mm; 13.91" ~ 18.58"
Width	487.3 mm (19.19")
Depth	166.0 mm (6.54")
Weight	
Weight (panel only - for VESA mount)	2.75 kg (6.06 lb)
Weight (with stand)	4.72 kg (10.41 lb)
Weight (with packaging)	6.26 kg (13.80 lb)
Standard Service Plan	Premium Panel Exchange, 3 Years Advanced Exchange Service[2] & Limited Hardware Warranty[7]
Optional Service Plan	Dell ProSupport[3]
Environmental Compliance	ENERGY STAR®, EPEAT® registered where applicable[10], RoHS Compliant, TCO-Certified Display, BFR/PVC free monitor (excluding external cables), Arsenic-Free glass and Mercury-Free for the panel only

What's in the box?

Components
- Monitor with stand

Cables
- DisplayPort cable
- USB 3.0 upstream cable
- Power cable

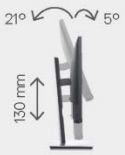
Documentation
- Quick Setup Guide
- Safety and regulatory information

Adjustability and connectivity

DELL 22 MONITOR | P2219H

Easily adjust the panel to your preferred viewing position.

Back view -
Cable management slot



Tilt and height adjustable

Pivot

Swivel

Connectivity

- **A** Power connector
- **B** HDMI port
- **C** Stand lock feature
- **D** DisplayPort
- **E** VGA connector
- **F** USB upstream port
- **G** USB downstream ports (x2)
- **H** USB downstream ports (x2)

RECOMMENDED ACCESSORIES

DELL DUAL MONITOR STAND | MDS19

Enjoy toolless monitor installation with Quick Release and the flexibility to pivot, tilt, swivel and adjust the height of each monitor independently. Features a small footprint and neat cable management.

DELL PRO STEREO SOUNDBAR | AE515M

Optimize conference calls and multimedia streaming with exceptional audio clarity. Minimize background noise with the dual mic array and echo-cancelling feature.

DELL WIRELESS KEYBOARD AND MOUSE | KM636

Elevated and spacious chiclet keys with muted typing sound. Pair up to 6 devices with Dell Universal Pairing.

1 Dell monitors are #1 Worldwide for 6 consecutive years (2013 to 2018)! Source: IDC Worldwide Quarterly PC Monitor Tracker, Q4 2018.
2 Advanced Exchange: Dell will send you a replacement monitor the next business day in most cases, if deemed necessary after phone/online diagnosis. Shipping times may vary by location and for monitors 55" and above. Fee charged for failure to return defective unit. See dell.com/servicecontracts/global.
3 Availability varies, please visit www.dell.com/support for details.
4 Based on Dell internal analysis comparing the area of the monitor base in Dell P2219H versus P2217H.
5 Source: Based on Principled Technologies Report commissioned by Dell, "Improve productivity with the new Dell P Series monitors in a dual-display configuration", November 2018, comparing Dell 24 USB-C Monitor – P2419H/HC and Dell 24 Monitor – P2414H/HC. Actual results will vary. Full report: https://www.principledtechnologies.com/Dell/P2419H_monitor_productivity_1118.pdf
6 TÜV Certified (ID0000051369–Flicker Free / ID0000051370–Low Blue Light Content). For more details, visit www.tuv.com.
7 For a copy of the Limited Hardware Warranty, write to Dell USA LP, Attn: Warranties, One Dell Way, Round Rock, TX 78682 or see dell.com/warranty.
8 Color gamut (typical) is based on CIE1976 (82%) and CIE1931 (72%) test standards.
9 Maximum power consumption with max luminance and contrast.
10 EPEAT registered where applicable. EPEAT registration varies by country. See www.epeat.net for registration status by country.

Dell.com/monitors Product availability varies by country. Please contact your Dell representative for more information.

v.3 03/2019