

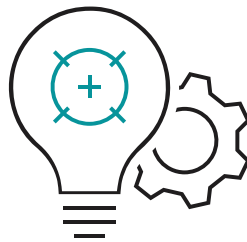


**F&C CPAs**



# RESOURCE KIT: ACCESS DENIED

Innovation & Expertise  
Upon History & Heritage



Casino Operations

# REMOTE ACCESS VIOLATION INCIDENT REPORT

This form is used to document and investigate unauthorized activities related to remote access to the network.

## Date of Report:

### Reported By:

- Name:
- Position:
- Department:
- Email:
- Phone number:

### Incident Details:

- Date & Time of Incident:
- Location (if applicable):
- Individual(s) Involved:

### Incident Description:

- Brief Description of Unauthorized Activity Observed:
  
- Detailed Description of Incident:

### Evidence Collected:

- System Logs:  Yes  No
- Screenshots:  Yes  No
- Communication Records:  Yes  No
- Other (Specify):

**Immediate Actions Taken:**

- Access Revoked:  Yes  No
- Individual Notified:  Yes  No
- IT Security Team Alerted:  Yes  No
- Legal/Compliance Notified:  Yes  No
- Other (Specify):

**Potential Impact:**

**Recommended Next Steps:**

**Final Review & Sign-Off:**

- Investigated By:
- Date of Completion:
- Approved By:
- Signature:

# Remote Access Tool List



## Virtual Private Networks (VPNs) – Secure Remote Access

- **Cisco AnyConnect** – Enterprise-grade VPN with strong security features
- **Palo Alto GlobalProtect** – Integrated with next-gen firewalls for advanced security
- **Fortinet FortiClient** – Secure VPN with endpoint security integration
- **OpenVPN** – Open-source VPN with customizable security options
- **NordLayer** – Business-oriented VPN with cloud security features



## Two-Factor Authentication (2FA) & Multi-Factor Authentication (MFA)

- **Duo Security (by Cisco)** – User-friendly MFA with device health monitoring
- **Microsoft Authenticator** – Integrated with Microsoft 365 for easy 2FA
- **Google Authenticator** – Simple app-based authentication for various logins
- **Okta Verify** – Cloud-based identity management and MFA
- **RSA SecurID** – Enterprise MFA with hardware and software token options



## Secure Remote Desktop & Access Management

- **TeamViewer Tensor** – Secure remote access with enterprise-grade security
- **AnyDesk** – Lightweight and fast remote desktop access tool
- **BeyondTrust Remote Support** – Secure remote access with privileged access management
- **LogMeIn Pro** – Encrypted remote access with file sharing and remote printing
- **Splashtop Business Access** – Secure, fast remote access with device authentication



## Endpoint Security & Monitoring Tools

- **CrowdStrike Falcon** – Endpoint detection and response with real-time monitoring
- **SentinelOne** – AI-powered endpoint security with automated response
- **Microsoft Defender for Endpoint** – Integrated security monitoring for Windows systems
- **Symantec Endpoint Protection** – Comprehensive endpoint security with remote management
- **Bitdefender GravityZone** – Cloud-managed endpoint protection with strong threat detection

# Remote Access Tool List



## Privileged Access Management (PAM) & Identity Security

- **CyberArk** – Enterprise-level privileged access management
- **BeyondTrust Privileged Remote Access** – Secure remote access for privileged users
- **Thycotic Secret Server (Delinea)** – Password vaulting and access control
- **One Identity Safeguard** – Secure access control for privileged accounts



## Network Access Control (NAC) & Zero Trust Solutions

- **Zscaler Zero Trust Exchange** – Cloud-based zero trust network access (ZTNA)
- **Cloudflare Zero Trust** – Secure remote work with application access control
- **Perimeter 81** – Zero trust network security for remote workforces
- **Tailscale** – WireGuard-based zero trust VPN for teams

# AUTO GENERATED ACTIVITY LOG

**Activity Log**  
 Sentry: Example Casino, Date: 09/01/24 - 09/30/24

ID	Sentry	Gate	Approver	Authorized User	Reason For Access	Work Performed	Begin Date	End Date	Duration
967178	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/30/24 12:01 am	09/30/24 11:59 pm	23:58
966922	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/29/24 12:01 am	09/29/24 11:59 pm	23:58
966703	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/28/24 12:01 am	09/28/24 11:59 pm	23:58
966449	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/27/24 12:01 am	09/27/24 11:59 pm	23:58
966200	Example Casino	VGT	Jone Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/26/24 12:01 am	09/26/24 11:59 pm	23:58
965918	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/25/24 12:01 am	09/25/24 11:59 pm	23:58
965669	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/24/24 12:01 am	09/24/24 11:59 pm	23:58
965417	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/23/24 12:01 am	09/23/24 11:59 pm	23:58
965189	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/22/24 12:01 am	09/22/24 11:59 pm	23:58
964917	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/21/24 12:01 am	09/21/24 11:59 pm	23:58
964636	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/20/24 12:01 am	09/20/24 11:59 pm	23:58
964337	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/19/24 12:01 am	09/19/24 11:59 pm	23:58
964098	Example Casino	VGT	Jone Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/18/24 12:01 am	09/18/24 11:59 pm	23:58
963852	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/17/24 12:01 am	09/17/24 11:59 pm	23:58
963607	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/16/24 12:01 am	09/16/24 11:59 pm	23:58
963357	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/15/24 12:01 am	09/15/24 11:59 pm	23:58
963114	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/14/24 12:01 am	09/14/24 11:59 pm	23:58
962873	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/13/24 12:01 am	09/13/24 11:59 pm	23:58
962628	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/12/24 12:01 am	09/12/24 11:59 pm	23:58
962372	Example Casino	VGT	John Doe	Health Monitor	Unattended(3388)	Health Monitoring for VGT	09/11/24 12:01 am	09/11/24 11:59 pm	23:58

# MANUAL ENTRY ACTIVITY LOG

REMOTE ACCESS LOG							
DATE	AUTHORIZATION	NAME/COMPANY	IN	OUT	PURPOSE OF ENTRY FOR ACCESS	CHANGES MADE	ACCESS TIME
7/8/2011	John Doe	Example Company	944	948	Pull ACT Reports	None	4m
7/13/2011	John Doe	Example Company	1136	1153	Error Check APP-01	None	17m
7/13/2011	John Doe	Example Company	1000	1200	Changed EWSM for Mail Traffic	Switch Configuration	2h
7/19/2011	John Doe	Example Company	1620	1720	Restore Service	Games online	1h
7/20/2011	John Doe	Example Company	800	1100	Pull ACT Reports	Switch Configuration	3h
7/26/2011	John Doe	Example Company	1129	1134	Check SDS Report Problem(Verden)	None	5m
7/26/2011	John Doe	Example Company	2034	2150	Theoretical Hold Reports	None	1h16m
8/2/2011	John Doe	Example Company	1101	1210	Hold Summary Report	None	1h9m
8/3/2011	John Doe	Example Company	1210	1237	Clear error on APP Server	None	27m
8/8/2011	John Doe	Example Company	948	1130	Pull ACT Reports	Error Cleared	42m
8/11/2011	John Doe	Example Company	1045	1105	Check Server APP-00 Status	None	20m
8/11/2011	John Doe	Example Company	1115	1123	Pull ACT Reports	None	8m
8/16/2011	John Doe	Example Company	1118	1125	Pull ACT Reports	None	7m
8/23/2011	John Doe	Example Company	1006	1012	Pull ACT Reports	None	6m
8/30/2011	John Doe	Example Company	935	940	Slot Points error	None	5m
9/5/2011	John Doe	Example Company	1140	1231	Pull ACT Reports	Fixed Slot Rating for S2 Slots	51m
9/15/2011	John Doe	Example Company	1439	1455	Pull ACT Reports	None	16m
9/19/2011	John Doe	Example Company	1008	1014	Pull Archive Files from Tape	None	6m
9/21/2011	John Doe	Example Company	1113	1516	eCash error	None/Failed	4h3m
9/22/2011	John Doe	Example Company	820	825	Soft count upload error	Restart eCash	5m
9/23/2011	John Doe	Example Company	1052	1225	Pull ACT Reports	None	1h38m
9/26/2011	John Doe	Example Company	938	952	MSG Build Problem	None	14m
9/26/2011	John Doe	Example Company	1730	1815	Check on CMP errors	None	45m
10/2/2011	John Doe	Example Company	1330	1540	Pull ACT Reports	None	2h10m
10/4/2011	John Doe	Example Company	1448	1453	Pull ACT Reports	None	5m
10/10/2011	John Doe	Example Company	1131	1141	Pull ACT Reports	None	10m
10/17/2011	John Doe	Example Company	902	1002	Pull ACT Reports	None	1h
10/24/2011	John Doe	Example Company	1137	1151	Pull ACT Reports	None	14m

REMOTE ACCESS LOG											
DATE	AUTHORIZATION	NAME/COMPANY	IN	OUT	PURPOSE OF ENTRY FOR ACCESS	CHANGES MADE	ACCESS TIME				
11/14/2011	John Doe	Example Company	944	948	Pull ACT Reports	None	4m				
11/15/2011	John Doe	Example Company	1136	1153	Error Check APP-01	None	17m				
11/15/2011	John Doe	Example Company	1000	1200	Changed EWSM for Mail Traffic	Switch Configuration	2h				
11/19/2011	John Doe	Example Company	1620	1720	Restore Service	Games online	1h				
11/20/2011	John Doe	Example Company	800	1100	Pull ACT Reports	Switch Configuration	3h				
11/26/2011	John Doe	Example Company	1129	1134	Check SDS Report Problem(Verden)	None	5m				
11/26/2011	John Doe	Example Company	2034	2150	Theoretical Hold Reports	None	1h16m				
11/2/2011	John Doe	Example Company	1101	1210	Hold Summary Report	None	1h9m				
11/3/2011	John Doe	Example Company	1210	1237	Clear error on APP Server	None	27m				
11/8/2011	John Doe	Example Company	948	1130	Pull ACT Reports	Error Cleared	42m				
11/11/2011	John Doe	Example Company	1045	1105	Check Server APP-00 Status	None	20m				
11/11/2011	John Doe	Example Company	1115	1123	Pull ACT Reports	None	8m				
11/16/2011	John Doe	Example Company	1118	1125	Pull ACT Reports	None	7m				
11/23/2011	John Doe	Example Company	1006	1012	Pull ACT Reports	None	6m				
11/30/2011	John Doe	Example Company	935	940	Slot Points error	None	5m				
12/5/2011	John Doe	Example Company	1140	1231	Pull ACT Reports	Fixed Slot Rating for S2 Slots	51m				
12/15/2011	John Doe	Example Company	1439	1455	Pull ACT Reports	None	16m				
12/19/2011	John Doe	Example Company	1008	1014	Pull Archive Files from Tape	None	6m				
12/21/2011	John Doe	Example Company	1113	1516	eCash error	None/Failed	4h3m				
12/22/2011	John Doe	Example Company	820	825	Soft count upload error	Restart eCash	5m				
12/23/2011	John Doe	Example Company	1052	1225	Pull ACT Reports	None	1h38m				
12/26/2011	John Doe	Example Company	938	952	MSG Build Problem	None	14m				
12/26/2011	John Doe	Example Company	1730	1815	Check on CMP errors	None	45m				
1/2/2012	John Doe	Example Company	1330	1540	Pull ACT Reports	None	2h10m				
1/4/2012	John Doe	Example Company	1448	1453	Pull ACT Reports	None	5m				
1/10/2012	John Doe	Example Company	1131	1141	Pull ACT Reports	None	10m				
1/17/2012	John Doe	Example Company	902	1002	Pull ACT Reports	None	1h				
1/24/2012	John Doe	Example Company	1137	1151	Pull ACT Reports	None	14m				



## The Ghost in the Machine: Remote Access Control

Remote access is no longer just a convenience—it's a necessity. But with every connection comes risk. Tribal Gaming operations must navigate the challenge of securing vendor access while staying compliant with MICS 543.20(h), a regulation that, despite its mere 87 words, leaves room for complexity and confusion. This article explores the evolving landscape of remote access, the gaps in regulatory guidance, and how GhostSentry provides a purpose-built solution to take back control, mitigate risks, and protect your network.

**Doug Parker**  
*Business Consultant*





*George Washington's second inaugural address – the shortest of any Presidential inauguration address – was 135 words. In 1998, Robin Williams won the Academy Award for Best Actor for his work in Good Will Hunting. His acceptance speech was 150 words. Taylor Swift's popular song Fortnight is a total of 199 words. Throughout history, people continue to find a way to say a lot even when using just a few words. It's an art!*

## The 87-Word Conundrum

The exception to this rule may be internal controls. Rarely, if ever, does the “less is more” philosophy apply with strong regulation. MICS 543.20(h) has a grand total of 87 words. If you are still reading this, you have read 112 words already – which means you have exceeded the total word count of the vital section of Information Technology *minimum* internal controls in our Tribal Gaming industry. Even in its simplicity, these 87 words continue to create challenges for both operations and vendors.

In fairness, these controls have not been updated in over 10 years. Technology is radically different than it was in 2012. The post-Covid world not only allows remote access, but it also often requires it. Regulating that access is challenging, to say the least.

For years, balancing the convenience of allowing vendors to remotely access equipment connected to the operation's network all while mitigating the risks and vulnerabilities that come with this technology has been a bit of a mystery. To complicate things further, the MICS offered up these 87 words to help “control” the risks but left enough ambiguity to create some chaos in the most appropriate way to log and monitor remote access.

---

*"The challenge isn't just about compliance; it's about ensuring long-term security and resilience."*

---

## From Chaos to Control: The Solution Emerges



From this chaos, GhostSentry was born. At the heart of the regulations, the operation should be protecting their network. 15 years ago, remaining in compliance with these regulations often meant a pen and paper log or a fancy spreadsheet where the information of who was accessing your network was recorded. The risk of missing the logging of a remote session became as great as the risk of the remote session itself. GhostSentry eliminates these risks! In simplistic terms, it serves as a firewall to keep remote traffic out of your network without proper authorization and approval.

The complexity of the system allows for flexible access for users and ongoing access to vendor equipment on a case-by-case basis or on an ongoing basis when approved by management. GhostSentry was intentionally developed as a solution to effectively control remote access in the gaming industry. It is the only such solution in this industry!

## Why It Matters: The Cost of Getting It Wrong

Data and information are as valuable as cash in the modern casino. In the past year alone, multiple casinos have suffered devastating cyber-attacks, bringing operations to a standstill. Any access point—including remote access—creates potential vulnerabilities that must be managed carefully. The challenge isn't just about compliance; it's about ensuring long-term security and resilience. GhostSentry was designed with this in mind, providing a streamlined way to control remote access, mitigate risk, and uphold the highest standards of regulatory compliance.

*"In an industry where data is as valuable as cash, securing remote access isn't just a best practice—it's a business imperative. By refining security measures and leveraging the right technology, Tribal Gaming operations can take control of their networks and stay ahead of evolving cyber threats."*

A business card for Doug Parker, Business Consultant at GhostSentry. The card features the GhostSentry logo on the left, which consists of a stylized figure in a circle above the text 'GHOSTSENTRY'. To the right of the logo, the text reads: 'Doug Parker BUSINESS CONSULTANT', 'Direct: 405-395-5106', 'Mobile: 405-401-9010', 'dparker@ghostsentry.com', and '601 N. Broadway Avenue Shawnee, OK 74801'. On the far right of the card is a photograph of Doug Parker, a man in a suit and tie, sitting and smiling.