SYSTEM ACCESS

VERSION2.0
PUBLISHED DECEMBER 2019

Table of Contents

REMOTE ACCESS FOR SYSTEM SUPPORT 3

UNABLE TO USE SPOK STANDARDIZED REMOTE ACCESS 3

SYSTEM ACCESS TYPES 4

SYSTEM ACCESS USER CREDENTIALS 6

Linux Credentials: 6

Oracle Credentials: 6

Windows Credentials: 6

SQL Credentials: 7

OTHER SYSTEM ACCESS REQUIREMENTS 7

Spok Support User Administration†: 7

Accessing systems and 24x7x365 Password Change Process†: 7

Short term new user add process†: 7

Two factor authentication†: 8

System Access notification: 8

Compliance Training: 8

Collection of application logs, system logs or Spok data: 9

Spok Employee Identification requirements: 9

Connectivity IP Ranges† 9

REMOTE ACCESS FOR SYSTEM SUPPORT

To quickly and accurately resolve issues, it is Spok's policy for a customer to provide Spok with remote access to all equipment where Spok products are installed on customer premise systems.

Spok has standardized on a remote access solution called SecureLink by SecureLink®. SecureLink is the chosen remote access solution for the nation's top hospitals. It provides a highly secure and configurable remote support solution utilizing two factor authentication that puts the customer in complete control of who is allowed access, when to allow access and what can be accessed while connected to your system. You may obtain more detailed information about the benefits and security capabilities of SecureLink from Spok's support staff or via the SecureLink website (www.securelink.com).

	SecureLink *Purpose-built for secure third-party remote access*	VPN *Great for internal employees, but struggles to identify, control and audit third parties*	Desktop Sharing *Great for attended desktop support and helpdesk, but lacks the security and functionality for complex enterprise remote support*
Access Control	✓	✓–	X
Multiple Operating Systems	✓	✓	X
Tools for Complex Remote Support	✓	✓	X
Collaboration	✓	X	✓
Proactive Customer Monitoring	✓	X	X
Single Sign-on (SSO)	✓	✓	X
Individual Identity Management	✓	✓–	X
Audit Capabilities	✓	✓–	X
Password Management	✓	X	X
Chat	✓	X	✓
CRM Integration	✓	X	✓–

UNABLE TO USE SPOK STANDARDIZED REMOTE ACCESS

Spok recognizes that system security is very important and takes the security of your system very seriously. It is equally important that customer's do not lock down Spok's access that may prevent Spok from providing the support needed to ensure timely issue resolution. While connected to the customer's system, Spok requires:

- The ability to perform file transfers to the customer's Spok systems
- Access and administrative rights to Spok desktops, workstations and servers

Important notes for alternative connection options
If policies prevent customers from allowing Spok to use SecureLink as the VPN, the customer will be responsible for any delays in service resolution response times.

SYSTEM ACCESS TYPES

Access Type	Access Description	Maintenance Impact	Other
Spok provided and preferred solutions			
SecureLink	Remote connectivity, utilizing two factor authentication enabling Support Engineers to troubleshoot issues. www.securelink.com	No additional charge to maintenance	Highly secure and customer configurable connection method
GoToAssist†	Remote Support Tool requiring customer collaboration to provide Two Way Screen Share, File Transfer, and Remote Diagnostics. Collaborative support method allowing customers to provide support access to customer's systems.	No additional charge to maintenance	Connection method requires users at the customer site to provide and approve access to supported systems real-time. Customer users must have access and administrative rights to Spok systems. Non-direct connections may delay recovery and patch installation.
Exceptions requiring Spok management approval			
B2B	Remote connectivity for Support Engineers to connect to customer systems to troubleshoot cases.	Spok will charge an initial setup fee and a line item will be added to your maintenance contract to maintain your dedicated tunnel	Initial fee and Increase in annual maintenance
VPN	Remote connectivity for Support Engineers to connect to customer's network and systems to troubleshoot Spok issues.	Spok will charge an additional line item to your maintenance contract for the use of a non SecureLink VPN. Each VPN solution will be	Increase in maintenance, some limitations apply

		assessed accordingly. If the VPN solution conflicts with our Spok network access, Spok reserves the right to decline the use of the VPN solution. Unaccepted VPN's: Cisco AnyConnect and Cisco VPN	
No Remote Access†	If customer is unable to provide remote access for security reasons and support is unable to resolve the issue, customers may: 1. Choose to send their equipment to Spok Support for continued troubleshooting. 2. Request Spok to come on location to resolve the issue, you will be charged the current daily rate plus travel expenses. This request is subject to availability.	No additional charge to maintenance	Customer is responsible for all shipping and travel costs and will be responsible for any damage to equipment that occurs during shipping.
Customer Provided collaboration tool (such as WebEx)†	Customer provided collaboration tool to provide Two Way Screen Share. Collaborative support method allowing customers to provide support access to customer's systems.	No additional charge to maintenance.	Connection method requires someone at customer site to provide and approve required access to supported systems. Customer users must have access and administrative rights to Spok systems.

SYSTEM ACCESS USER CREDENTIALS

Linux Credentials:

Preferred:

Non-Root user

- Shared user for Spok Support Staff
- Password does not expire
  - *Customer responsible to inform Spok of any password changes*

Root user

- Password does not expire
  - *Customer responsible to inform Spok of any password changes*
- *Spok can work with a Sudo user for basic troubleshooting, but direct root access may be required to resolve system issues such as paging and daemon restarts and for complex patch installations or upgrades.*

Oracle Credentials:

Preferred:

Spok Oracle user

- Shared user for Spok Support Staff
- Password does not expire
  - *Customer responsible to inform Spok of any password changes*
- Support user requires 'sysdba' privileges

Windows Credentials:

Preferred:

Windows Spok user

- Shared user for Spok Support Staff
- Password does not expire
  - *Customer responsible to inform Spok of any password changes*
- Support user requires 'local administrator access' to all Spok Windows Servers

Unique login requirements for Windows:

Customers who require unique logins for each specific support engineer:

- Customer is responsible to ensure that Spok unique users have 'local administrator access' to all Spok Windows Servers
  - *See "Accessing systems and 24x7x365 Password Change Process" below.*

SQL Credentials:

Preferred:

SQL Spok user

Shared user for Spok Support Staff

Password does not expire

Customer responsible to inform Spok of any password changes

Support user requires 'SA' to all Spok SQL instances

Unique login requirements for SQL:

Customers who require unique logins for each specific support engineer:

Customer is responsible to ensure that Spok unique users have 'SA' to all Spok Windows Servers

OTHER SYSTEM ACCESS REQUIREMENTS

Spok Support User Administration†:

- Customer is responsible to provide an email address for Spok to notify them of Support staff changes (Add, Remove).
- Spok will send an email notification to customers that require unique logins for all support staff.
- Customer will be responsible for ensuring Spok Support users are added or removed to all necessary Spok systems and that they have the appropriate system security rights.
- Customer is responsible to ensure any administration process is repeatable, sustainable and scalable.

Accessing systems and 24x7x365 Password Change Process†:

- Spok Support will only connect to customer servers to troubleshoot a support case or issue.
- Customer is responsible to provide Spok support with a 24x7x365 standard password change process in the event Spok Support is unable to connect due to an expired password.
- Spok Support will not connect to a customer system for the sole purpose of changing a password.

Short term new user add process†:

- Customer is responsible to provide Spok with a standard process to add temporary non-support users in the event additional Spok employees (Development or Services) require access for troubleshooting.

Two factor authentication†:

- Spok support uses two factor authentication when connecting to customers systems through SecureLink.
- Spok support can work with two factor authentications outside of SecureLink by utilizing Spok email as delivery of the 2nd factor. Spok uses an email security filter which will require additional setup to ensure email delivery.
- If a customer's two factor solution doesn't allow for email, the customer will be responsible for providing Spok support with any and all devices (including cell phones) or tokens needed to enable authentication and access. All physical devices will be stored securely in our Technology Operations Center and will only be utilized by Support staff when access is required to troubleshoot issues.
- Customer is responsible for providing the appropriate number of devices required for all Support Engineers.
- Customer is responsible for the ongoing maintenance and accounting of physical devices including updates require for changes in Support Staffing (Add, Remove).
- Spok support is not able to install any customer specific mobile authentication applications on Spok support devices.
- If a non-physical device option is available, the customer will provide Spok support with the appropriate 24x7 process for access.

System Access notification:

- Spok will make every effort to request permission from customers before accessing their systems. There may be times during critical troubleshooting where we may not be able to reach a customer prior to access. For customers using SecureLink, all access attempts by a Spok employees will be clearly documented.

Compliance Training:

With Spok's core business in the healthcare and government sectors, Spok ensures a rigorous compliance annual certification program. This program starts with hiring where Spok does an extensive background check to ensure all employees meet HIPAA and governmental requirements. Spok requires all existing employees to take annual HIPAA compliance trainings

With approximately 4 hours of annual mandatory security and compliance training, we ensure that our resources are always up to date on the latest regulatory requirements and associated best practices.

Providing our employees with a rigorous curriculum ensures that we are compliant to all customer needs for security and compliance requirements and therefor eliminates the need for individual customer training.

Specific certification data can be provided to our customers upon request to ensure that all the Spok Support Engineers are up to date with their certifications.

Collection of application logs, system logs or Spok data:

- As part of troubleshooting an issue, it may be necessary for Spok to collect application and/or systems logs for further analysis by other Spok teams such as development or Professional Services.
- If Spok is unable to reproduce an issue in-house, we may request a copy of the customers Spok database for internal testing.
- Spok utilizes Microsoft's encrypted OneDrive to securely collect and store customer secure data.
- Spok will provide the customer with a OneDrive secure share where the requested logs or data can be securely stored.
- Once troubleshooting is complete and the data is no longer needed, the share and data will be deleted.
- Spok will not collect any customer specific data without the permission of the customer.

Spok Employee Identification requirements:

Spok will complete the documents for security and access policies on behalf of Spok and its employees. Unique identifying information will be provided for each employee that requires access, however personal information such as date of birth, social security number, home address, etc. will not be provided. Based on the complexity of your security requirements, Spok may charge an additional Maintenance Fee to administer your on-going system security access requirements at Spok.

Connectivity IP Ranges†

The on-call engineers will need access from an IP range outside that of Spok's core office range. Access within other IP ranges must be allowed in order to connect. If this is not permitted and alternate arrangements need to be made to connect to your system, issue resolution times may be delayed.

† Spok is not responsible for any delays in recovery caused by failures in the above processes