# Providing Secure Remote Service and Support

Kevin Phillips, Security Services Project Manager for Teradata Customer Services

11.14 EB8537 CUSTOMER SERVICES

TERADATA.

## Table of Contents



## Teradata's Commitment

Teradata believes that privacy and security are of the highest importance to its customers and their end-user customers. Teradata maintains the following security principles:

- Protect the integrity of the system—network, equipment, and data
- Track access and activity to achieve regulatory compliance
- Provide flexibility and control to enforce business policies
- Audit and certify Teradata processes and solutions regularly by a third party

## Demand a Proven Methodology for Providing a Secure Connected Products Service

Employing remote services in a world where the complexity and velocity of threats continues to rapidly increase requires advanced security at all levels. It's imperative to deploy a proven remote service solution that protects against viruses and hackers without major end-user modifications. The right solution should also extend the current network security model so it can meet critical certification and compliance requirements while allowing the customer to maintain full control of access to their system. Because the manufacturer's devices are connected to their customer networks, end customers also need to be assured that the connected product supports their security model, provides granular control over user access, and offers easy-to-use audit and tracking capabilities to know precisely who, when and for how long someone is accessing their system.

To address key information security concerns, a remote service solution should have features that include the ability to:

- **Maintain network security at customer sites**. The solution leverages the customer's existing security infrastructure, using communication that works well with firewalls.
- **Conceal data from unauthorized parties**. All communication between you and your customers is kept secure using Transport Layer Security (TLS) encryption—the same method banks use for secure online transactions.
- **Ensure that system users are authenticated**. All access to the system is centrally controlled, requiring password authentication. All user actions are fully audited for traceability.
- **Limit each user to specific data, views, and actions.** Once authenticated, user actions are limited to the products for which they are responsible, and the level of access appropriate to their roles.

These well-documented operational standards should include a number of typical components, such as incident management, security monitoring, security awareness and training programs, and risk management and business continuity planning. They should also include change and

configuration management, capacity planning, and proactive threshold monitoring of core resources.

These processes should also be aligned with Information Technology Service Management (ITSM) best practices so customers can be assured their products and data are secure. The ITSM process has been thoughtfully designed as a component of the Information Technology Infrastructure Library (ITIL) standard.

### Application Security Perspective—Meeting Manufacturers' Most Stringent Requirements for Remote Service Security

Your remote service should meet the most stringent security requirements of manufacturers and end customers so that they can achieve broad adoption and maximum use of connected products—instilling confidence that their connections are secure and private. Some of the most common manufacturer requirements include:

- Enterprise proven design—connecting any computer to the Internet raises security concerns, and connecting intelligent devices is no different. Whether hackers are trying to harm a device with corrupt data or viruses, steal data traveling between the device and manufacturer, or gain unauthorized access to critical information, a connected product solution must guard against these and other threats.
- Rapid deployment—for customers to adopt remote service systems, the security capabilities must exist within the customer's current network security model.
- Support for multiple devices—manufacturers need to securely support a nearly infinite number of device types and complex customer configurations without requiring major end-user changes.

## End-Customer Requirements for Remote Service Security

Intelligent devices are connected to your customers' networks. Each customer has their own security policy and network protection in the form of firewalls, proxy servers, and addressing schemes. A device connected to their network will be protected behind these layers of security. If a connected product offering requires changes to your customer's network protection, it will likely fail to gain acceptance. That's why it is important to consider the requirements of the end customer, which include:

- Maintain the current security model—the manufacturer's device must support the way that the organization manages security operations, policies, or procedures, and should adhere to accepted industry standards.
- Control user access—in line with the customer's security model, the manufacturer's device must provide the customer—not the manufacturer—with granular control and set policies about the actions that can be performed on the device, such as data collection and software updates, and when those actions can be performed. These policies need to be centrally defined for all devices at a customer location.
- Audit and track activity—policy and regulatory compliance requirements dictate that the system must make auditing and tracking all users and administrative activity easy.

Teradata ServiceConnect™ delivers the performance, flexibility, and scalability required to meet the needs of the broadest range of device manufacturers by providing the widest range of data protection safeguards and security features.

## Requires Only Minimal or No Changes to IT Security Infrastructure

Teradata ServiceConnect™ uses a patented Firewall-Friendly™ technology that provides two-way communication based on Web Services standards, including Hypertext Transfer Protocol (HTTPS), Simple Object Access Protocol (SOAP), and eXtensible Markup Language (XML). For easier installation and operation in supporting remote monitoring and diagnostics, Teradata ServiceConnect™ requires only minimal or no changes to the IT security infrastructure of the end customer. In addition, communication between the data center of the manufacturer or service provider and the customer site is encrypted using Transport Layer Security (TLS) up to 168 bits using a 2048-bit RSA key. Packets within the tunnel are encrypted using 256-bit AES content encryption.

## No VPN or Modem Needed

The agent initiates all communications in compliance with the secure computing environment at the device site, so devices do not require public IP addresses and are not visible from outside the firewall. This makes for easier deployment and addressing compliance objectives because customers don't have to make changes to firewall settings or proxy servers. There is also no need to set up expensive VPNs to implement Teradata ServiceConnect™ or to compromise security by using dial-up communications. The only requirement is an Internet connection to the machine where the agent resides.

## Teradata ServiceConnect™ End-to-End Security Highlights

- Security certified
- Firewall-Friendly Communications™
- Complete end-customer control to enforce business policies
- HTTPS, PKI, and 128-bit TLS encryption data protection using 2048-bit RSA key
- AES 256-bit packet encryption
- No VPN or modems needed
- Minimal or no changes required to IT and security infrastructures
- Easy to deploy and manage user, application, and device security

## Establish and Enforce Device Security and Data Privacy Policies

Teradata ServiceConnect™ Policy Server is a core security component of Teradata ServiceConnect Enhanced™. It is a software application that enables authorized customer administrators to establish and enforce the privacy

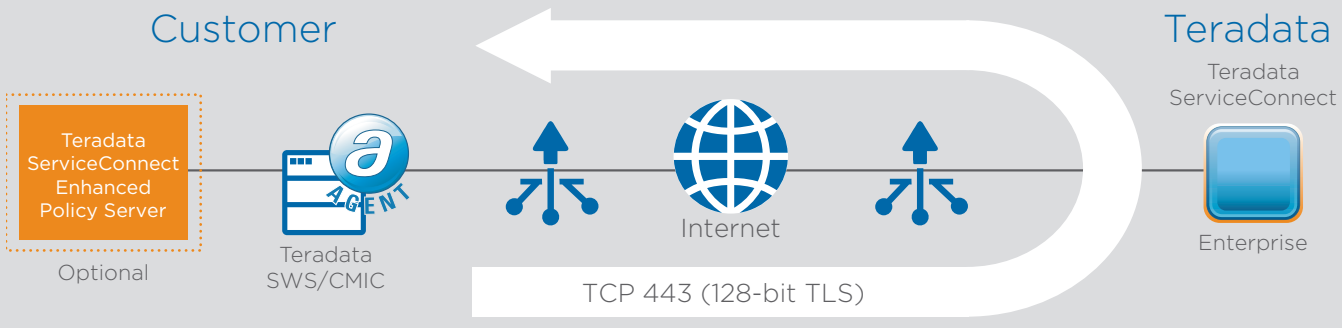


Figure 1: Teradata ServiceConnect™ Communication

policy for all of their devices in a single place. Teradata ServiceConnect™ Policy Server resides on the customer's network, providing a comprehensive and granular set of permission settings that continuously govern behavior. This governance includes which types of data and files can leave the device, and which activities the manufacturer can conduct on the device. Control can be automatic, based on the policy, or configured to notify the customer that an action request is pending.

## Easily Manage Enterprise User Authentication and Access Control

The Teradata ServiceConnect™ system uses RSA two-factor authentications to authenticate Teradata remote users. User access control is added through activity-based access control and asset-based access control. These methods are combined in a variety of ways to allow users to do their jobs effectively while protecting access to sensitive information.

Activity-based access control enables the system administrator to assign and classify users in Teradata ServiceConnect™ and define the activities that can be performed.

Asset-based access control provides a method for defining the specific assets accessible to each user group, limiting the view of asset information to only those assets for which a user is responsible.

## Secure Communications and Data Confidentiality

Much of the information that travels across the public Internet uses plain text encapsulated within standard HTTP messages. Hackers can gain access to the network at a point close to the source or destination of the message, and then capture and view the text of these HTTP messages with readily available tools.

By default, Teradata ServiceConnect™ uses 128-bit TLS with 2048-bit RSA key. Teradata ServiceConnect™ also uses secret key AES 256-bit message encryption, which may be used with TLS to encrypt data beyond the demilitarized zone (DMZ). Proven standards-based communications also help with compliance with regulatory requirements.

Key security items Teradata ServiceConnect™ provides as standard include:

- Double Data Encryption
  - Web traffic utilizes 128-bit TLS encryption (tcp port 443)
  - Data inside the packets is encrypted with AES256 bit encryption
  - Data encryption can be disabled upon customer request, but TLS encryption cannot be turned off
- Support for HTTP and SOCKS proxy servers
- TLS certificates are issued by an industry-leading third party and are generated with a 2048 bit RSA key
- URI blocking only allows agent communication to specific locations within serviceconnect.teradata.com
- Agent account is required to register with the enterprise server
- The optional policy server provides complete customer control
- Requires only one outbound port to be opened

## Proven Deployments Around the World

Teradata ServiceConnect™ is deployed around the world by manufacturers in a range of industries, including communications, finance, government, healthcare, manufacturing, media & entertainment, oil & gas, retail, travel & transportation, and more. These industry leaders rely on Teradata and Teradata ServiceConnect™ to enable their service organization to provide secure, remote business-critical services by incorporating end-to-end security strategies covering all levels, including network, application, user, and data security.

## TERADATA SECURITY FEATURES AND BENEFITS

### Network Security

Features:

- Firewall-Friendly™ technology is based on Web Services standards, including HTTPS, SOAP, and XML.
- Teradata Agent initiates all communication, so devices do not require public IP addresses and are not visible from outside the firewall.

Benefits:

- Customers don't have to make changes to firewall settings or proxy servers, easing deployment and addressing compliance objectives.

### System and Data Security

Features:

- TLS encryption supports key length up to 168 bits and mutual authentication using bi-directional digital certificates.

Benefits:

- Only authorized parties have access to designated devices and data. End customers can limit access, views, and even actions based on the user's role, which gives them control over users and actions.
- Proven standards-based communications help with compliance with regulatory requirements.

## Summary

For customers or end users employing remote services, security and privacy are primary concerns and will continue to be ever more challenging as attackers and threats evolve. Organizations throughout the world are providing safe, secure remote services to their customers using Teradata ServiceConnect™. Teradata ServiceConnect™ delivers the performance, flexibility, and scalability required to meet the needs of the broadest range of device manufacturers by providing the widest range of data protection safeguards and security features. Security principles and standards have been carefully incorporated in the design and operation of the Teradata infrastructure and services. A top priority at Teradata, stringent security enables our customers to achieve their remote service goals—securely and efficiently.

## About Teradata

Teradata is a global leader in analytic data platforms, marketing and analytic applications, and consulting services. Teradata helps organizations collect, integrate, and analyze all of their data so they can know more about their customers and business and do more of what's really important. With 10,000+ professionals in 77 countries, Teradata serves more than 2,500 customers, including the top companies across all major industries: consumer goods, financial services, healthcare, automotive, communications, travel, hospitality, and more. An ethical and future-focused company, Teradata is recognized by the business media and industry analysts for technological excellence, sustainability, and business value. Visit **Teradata.com** for details.

10000 Innovation Drive, Dayton, OH 45342 **Teradata.com**



11.14 EB8537

TERADATA