SupportAssist Enterprise Version 4.0

Technical Description Guide

Abstract

This document provides a technical overview of SupportAssist Enterprise.

May 2020

Table of contents

1 Introduction

SupportAssist Enterprise is a service capability that enables automated support from Dell EMC by remotely identifying hardware issues in your IT environment. SupportAssist Enterprise enables Dell EMC to identify, diagnose, and resolve hardware issues faster, thereby eliminating or reducing downtime. SupportAssist Enterprise monitors alerts from your devices without increasing the load on your network. When one or more alerts indicating a critical failure are detected, a service request is automatically submitted to Dell EMC, saving valuable time for you and your IT department. SupportAssist Enterprise delivers a secure, IP-based, distributed remote service support solution that provides command, control, and visibility of remote services access.

SupportAssist Enterprise Version 4.0 is the virtual edition of SupportAssist Enterprise.

The following are the benefits of SupportAssist Enterprise:

- Improved service levels
- Increased protection of information
- Simplification of complex environments
- Reduced risk
- Improved time-to-repair

1.1 Security

SupportAssist Enterprise incorporates the industry-recognized “3 As”: authentication, authorization, and audit logging. SupportAssist Enterprise is an asynchronous messaging system in which all communications are initiated from your site. All communications between SupportAssist Enterprise and the backend use the HTTPS protocol with end-to-end TLS tunneling with strong encryption.

SupportAssist Enterprise uses a firewall-friendly, IP-based communication technology over TLS VPN tunnels. The server on which SupportAssist Enterprise is deployed negotiates the secure exchange of information between the devices and the backend. All communication between your site and the backend is initiated by the server on which SupportAssist Enterprise is deployed. Using industry standard Transport Layer Security (TLS) encryption over the Internet, and Dell EMC-signed digital certificate authentication, your administrators need to enable outbound communication over TLS default ports 443 and 8443.

NOTE: If port 8443 is not open, the time taken by SupportAssist Enterprise to resolve issues on the end devices is affected.

SupportAssist Enterprise is scalable, fault-tolerant, and provides you with authentication, authorization, and audit logging control. A session-based IP port-mapping solution is used to remotely access your devices. Service notification files are transferred from the managed devices through the server on which SupportAssist Enterprise is deployed to ensure secure encryption and audit logging.

SupportAssist Enterprise comprises a suite of software products that securely link your devices to the backend. This distributed system provides you with the commands and controls to authorize and log support actions such as remote access connections, file transfers, diagnostic script executions, and system updates.

NOTE: The support actions are not available for all the devices that are supported by SupportAssist Enterprise.

SupportAssist Enterprise follows the enhanced security practices and encryption technologies, including:

- Advanced Encryption Standard (AES), SHA-2, 256-bit encryption between SupportAssist Enterprise and the backend
- Bilateral certificate authentication for all communication between the Client and the backend
- Configurable security between SupportAssist Enterprise components
- Customer Multifactor Authentication while registering SupportAssist Enterprise

1.2 Licensing usage data

Devices can send licensing usage data to the backend over a secure channel through the REST APIs. The data is stored for monitoring and reporting across all supported devices at all customer locations.

1.3 Updates

SupportAssist Enterprise automatically detects availability of updates and notifies users through the web user interface and email when any new update is available.

2 Customer site components

This section describes the SupportAssist Enterprise components at the customer site.

2.1 SupportAssist Enterprise Virtual Edition

SupportAssist Enterprise can be deployed on a customer-supplied VMware ESX or Microsoft Hyper-V instance. It can also be installed on multiple virtual infrastructure servers (two or more servers are preferred for high availability (HA). The servers act as the single point of entry and exit for all IP-based remote services activities and most Connect Home notifications. In an HA configuration, one or more servers monitors the same devices but do not communicate with each other.

SupportAssist Enterprise functions as communications broker between the managed devices, the Policy Manager, and the backend. All communication with the backend initiates from SupportAssist Enterprise on port 443 or 8443 outbound. The servers on which SupportAssist Enterprise is deployed are HTTP handlers. All messages are encoded using standard XML and SOAP application protocols. SupportAssist Enterprise message types include:

- Device state heartbeat polling
- Data file transfer (Connect Homes)
- Licensing Usage Data transfer (using MFT RESTful Webservices)
- User authentication requests
- Device management synchronization

Each server on which SupportAssist Enterprise is deployed acts as a proxy, carrying information to and from managed devices. SupportAssist Enterprise can also queue Connect Home events in the event of a temporary local network failure. The servers on which SupportAssist Enterprise is deployed have their own web user interface, which is run on the underlying OpenSUSE operating system (runs as Linux Service). All SupportAssist Enterprise actions are logged to a local runtime and audit files.

SupportAssist Enterprise polls the Policy Manager, receives the current policies, and caches them locally. During the periodic poll, SupportAssist Enterprise posts all requests and actions that have occurred. These are written to the Policy Manager database and the Policy Manager audit log files.

2.2 Policy Manager

Policy Manager enables you to set permissions for the following devices or device models that are managed by SupportAssist Enterprise:

- Data protection
- Data storage devices other than the PeerStorage (PS) or Equallogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models
- Converged infrastructure appliances other than WebScale
- Hyperconverged infrastructure appliances

When the server on which SupportAssist Enterprise receives a remote access request from the backend, the access is controlled by the policies that are configured on the Policy Manager.

It is recommended to install the Policy Manager software on a different server than the server on which SupportAssist Enterprise is deployed.

3 Communication between SupportAssist Enterprise and the Dell EMC backend

All communication between the customer's site and the backend is initiated outbound from the customer's site by SupportAssist Enterprise. Using industry-standard Transport Layer Security (TLS) encryption over the Internet and Dell EMC-signed digital certificate authentication, SupportAssist Enterprise creates a secure communication tunnel.

SupportAssist Enterprise use industry-accepted bilateral authentication for the backend servers and the SupportAssist Enterprise. Each SupportAssist Enterprise server has a unique digital certificate, which is programmatically generated and installed during the deployment and activation and is verified by EMC whenever SupportAssist Enterprise attempts to contact the backend. SupportAssist Enterprise then verifies backend server certificate. Only when the mutual TLS authentication is passed, the messages are transmitted to the backend, securing the connection against spoofing and man-in-the-middle attacks.

The server on which SupportAssist Enterprise is deployed uses the TLS tunnel for the following functions:

- Heartbeat polling
- Remote notification
- Remote access

Each function relies on the TLS tunnel. However, communication processes and protocols within the tunnel vary by function.

3.1 Heartbeat polling

The Heartbeat is a regular communication, at a default interval of 1 minute, from SupportAssist Enterprise to the backend. Heartbeat polling is applicable only for the following devices or device models:

- Data protection
- Data storage devices other than the PeerStorage (PS) or Equallogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models
- Converged infrastructure appliances other than WebScale
- Hyperconverged infrastructure appliances

Each heartbeat contains data that identifies the server on which SupportAssist Enterprise is deployed and provides the connectivity status information of the devices. The heartbeat can also be used for transferring files to the backend from the devices.

3.2 Remote notification

The Remote notification function is also called the Connect Home function. SupportAssist Enterprise serves as a conduit for the devices to send event files to the backend. Errors, alerts, warning conditions, health reports, configuration data, and script execution statuses may be sent from the device to the backend.

When an alert is generated, an event message file is generated and sent to SupportAssist Enterprise. The file is received by SupportAssist Enterprise through one of the following listener services:

- HTTPS
- SMTP or email
- SupportAssist Enterprise REST Client
- Passive FTP

SupportAssist Enterprise compresses the file and sends it to the backend through the TLS tunnel and deletes the file from the listener directory. The file is then decompressed in the backend for analysis by the Technical Support teams.

SupportAssist Enterprise can also send the files to the backend through the SupportAssist Enterprise REST Client or during Heartbeat polling. You can also configure SupportAssist Enterprise to use the failover channels namely FTPS or customer email server.

3.3 Remote access

Dell EMC Technical Support can remotely access the devices to troubleshoot issues or perform device-specific actions. The remote access functionality is available only for the following devices or device models:

- Data protection
- Data storage devices other than the PeerStorage (PS) or Equallogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models
- Converged infrastructure appliances other than WebScale
- Hyperconverged infrastructure appliances

SupportAssist Enterprise uses asynchronous messaging to ensure that the remote access session is initiated from the customer site. After the session is authenticated in the backend, a Technical Support agent makes a request to access the device. The remote access session request includes the following:

- Unique identifier for the user
- Serial number of the device
- Name of the remote application to be run on the device
- Service request number if available.

The remote access request is queued in the backend until SupportAssist Enterprise sends the device's heartbeat to the backend and retrieves the work request.

In response to the Heartbeat XML message, the backend sends a special status in the SOAP response. This response contains the request information and the address of the Global Access Server and a unique session ID that SupportAssist Enterprise would use to connect. SupportAssist Enterprise uses its local repository to determine the local IP address of the device. It then checks with the cached policy from Policy Manager to see if the connection is permitted. If there is no cached policy, then SupportAssist Enterprise checks with the Policy Manager. If the connection is permitted, then SupportAssist Enterprise establishes a separate persistent TLS connection to the Global Access Server of the preferred port 8443 for the specific remote access session.

This secure session enables IP traffic from the Dell EMC Technical Support agent to be routed through SupportAssist Enterprise to the device. IP socket traffic that is received by the Global Access Server for this session is established, wrapped in a message, and sent to SupportAssist Enterprise.

SupportAssist Enterprise unwraps the SOAP object and forwards the traffic to the IP address and port of the end device for which the session was established. SOAP communication flows between SupportAssist Enterprise and the Global Access Server through this tunnel until it is terminated or times out after a period of inactivity.

As the result of an application remote access session request, SupportAssist Enterprise forwards the traffic to the specific ports at the IP address that is associated with the registered serial number of the device.

If a Policy Manager is configured, then these actions and requests are sent to the Policy Manager as audits, which are viewable in the Policy Manager web user interface and in the Policy Manager audit logs.

4 SupportAssist Enterprise configuration choices

A cluster refers to the relationship created on the SupportAssist Enterprise infrastructure between two or more servers on which SupportAssist Enterprise is deployed. Device management through cluster configuration is available only for the following devices or device models:

- Data protection
- Data storage devices other than the PeerStorage (PS) or Equallogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models
- Converged infrastructure appliances other than WebScale
- Hyperconverged infrastructure appliances

This section provides details on the configurations of SupportAssist Enterprise.

4.1 Server client configuration

SupportAssist Enterprise servers can be implemented in one of several configurations to meet your network and security requirements.

It is recommended that the operating systems of your Policy Manager servers be hardened before installing the Policy Manager software. The preparation and hardening of servers is the customer's responsibility.

There are no technical restrictions on the network location of the server on which SupportAssist Enterprise is deployed. It must connect to your devices, to Policy Manager, and to the backend. It is recommended that you use a firewall to block network ports not required by SupportAssist Enterprise.

The following table provides the various configuration choices and the number of virtual appliances that are required for the configuration:

Table 1 - SupportAssist Enterprise configuration choices

Configuration	Appliance Quantity
Single SupportAssist Enterprise*, no Policy Manager	One
Single SupportAssist Enterprise* and Standalone Policy Manager	Two
High-Availability SupportAssist Enterprise(s)**, no Policy Manager	Two
High-Availability SupportAssist Enterprise(s)** and Standalone Policy Manager	Three

* Do not place SupportAssist Enterprise or storage files on Dell EMC devices that are managed by SupportAssist Enterprise.
** HA SupportAssist Enterprise should run in separate customer virtual environments.

4.2 High Availability SupportAssist Enterprise cluster configuration

It is recommended to deploy a High Availability SupportAssist Enterprise cluster configuration to improve remote access accessibility and eliminate single point of failure. High availability clusters can be created only for the following devices or device models:

- Data protection
- Data storage devices other than the PeerStorage (PS) or Equallogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models
- Converged infrastructure appliances other than WebScale
- Hyperconverged infrastructure appliances

4.2.1 Synchronization of clusters

The various servers in a cluster are synchronized during polling cycles to ensure that the changes are automatically updated on all the SupportAssist deployments. When you add, delete, or edit a device, a synchronization message is sent to all the servers in a cluster. If a server in a cluster is not available during synchronization, it is synchronized when a successful poll message is received from the server.

4.2.2 Installing a High Availability SupportAssist Enterprise cluster

A High Availability cluster is created by your Technical Support agent. By default, your organization name followed by “HA” is assigned as the cluster name. You can assign a different name for the cluster, if required.

NOTE: You must not assign the same name for two servers in a cluster.

The High Availability cluster takes on the devices that are managed by SupportAssist Enterprise that is deployed on the first server that is enrolled in the cluster. When more servers are added to the cluster, they start managing the cluster’s devices.

NOTE: The first server used to create a High Availability cluster may have managed devices. Any additional server that is enrolled in a High Availability cluster must not be managing devices at the time of enrolment. An error message is displayed if SupportAssist Enterprise deployed on the additional server is managing devices.

5 Security features

This section details the security features of SupportAssist Enterprise.

5.1 Policy Manager

Policy Manager enables you to control the authorization requirements for remote access connections, diagnostic script executions, and other related activities. You can also set access permissions for the following devices or device models monitored using SupportAssist Enterprise:

- Data protection
- Data storage devices other than the PeerStorage (PS) or Equallogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models
- Converged infrastructure appliances other than WebScale
- Hyperconverged infrastructure appliances

SupportAssist Enterprise regularly polls Policy Manager for changes to the permissions and caches the permissions locally. All requests and actions are recorded in the Policy Manager database and local audit log files. When SupportAssist Enterprise receives a request for remote access or any other action, it enforces the policy that is received from the Policy Manager cache even if the Policy Manager is unavailable.

Policy Manager permissions can be assigned in a hierarchical system, establishing policies based on device types or specific models in a device type. For more information about the Policy Manager functions, see the Policy Manager Operations Guide available here.

When you set an authorization rule to ask for approval, the Policy Manager sends an email message to the designated address for each action request, per transaction. The email contains the action request itself and the user ID of the Technical Support agent.

The email also requests your permission to perform the action. Use the Policy Manager web user interface to accept or deny the requested action. You can create filters to set further restrictions on authorization and actions.

Since the Policy Manager's permission rules are cached at startup, SupportAssist Enterprise polls the Policy Manager for configuration updates. The Policy Manager rule set cache is automatically updated with the configuration updates after its last polling cycle. The Policy Manager is an HTTPS listener, which must be configured to receive messages on an agreed-upon port. The default port is 8443, but if required, you can specify a different port during your Policy Manager installation.

The Policy Manager uses the Apache Tomcat engine and a 100 percent compliant local JDBC relational database to provide a secure web-based user interface for permission management.

5.2 Logging

The Policy Manager records all remote services events, remote access connections, diagnostic script executions, and support file transfer operations and stores them in the Policy Manager database and flat text audit log files. The Policy Manager also audits access to the Policy Manager, policy changes, and all authorization or denial of access activities. The audits are viewed through the Policy Manager web user interface and cannot be edited. The audits are also streamed to local flat text files which can be read with any text editor and are not tamper proof. Audit logs can also be configured to stream to a syslog server in your environment.

5.3 Device control

You have complete control over the devices that are managed through SupportAssist Enterprise. You can create device groups based on device type, administrator group, organization or business unit, physical location of the device, or any other criteria. All device management operations are logged and must be approved in the backend by a Technical Support agent. A Technical Support agent approval is required only for device management operations for the following devices or device models:

- Data protection
- Data storage devices other than the PeerStorage (PS) or Equallogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models
- Hyperconverged infrastructure models other than Web Scale

5.4 Digital certificate management

While deploying SupportAssist Enterprise, the required digital certificates are also installed and are protected using unique password encryption. All messages that are received by SupportAssist Enterprise after registration, requires entity-validation authentication.

Digital Certificate Management automates the enrolment of the digital certificate through the RSA SecurID Authenticator and the Dell EMC's private certificate authority (CA). Digital Certificate Management enables programmatic generation and authentication of each certificate request. It also ensures that the certificate is issued and installed on the server on which SupportAssist Enterprise is deployed.

The digital certificate is a proof-of-identity of SupportAssist Enterprise that is deployed on your server. The certificate binds the identity of the server on which SupportAssist Enterprise is deployed to a key pair that is used to encrypt and authenticate communication with the backend. The Dell EMC's Certificate Authority is the central repository for the SupportAssist Enterprise key infrastructure.

After a request is made, the following steps are involved in issuing a certificate by the certificate authority:

1. The customer, Technical Support agent, or partner requesting the certificate are authenticated.

   NOTE: A Technical Support agent is authenticated using the RSA SecurID and is also verified if he or she is permitted to request a certificate. A customer is authenticated using his business enterprise account.

2. SupportAssist Enterprise gathers all the information that is required for requesting certificates.
3. A certificate request, private key, and a password for the private key are generated.
4. The certificate request information is saved in a request file to ensure that the information is accurate and complete.
5. The request is submitted over a TLS tunnel.
6. After the certificate is issued, it is automatically installed on the server on which SupportAssist Enterprise is deployed.

   NOTE: Authentication using RSA Lockbox technology ensures that the certificate is not copied and used on another machine.

6 Related SupportAssist Enterprise documents

In addition to this guide, you can see the following documents for more information about SupportAssist Enterprise 4.0. To access the documents, go to https://www.dell.com/serviceabilitytools.

- SupportAssist Enterprise Version 4.0 User's Guide
- SupportAssist Enterprise Version 4.0 Support Matrix
- SupportAssist Enterprise Version 4.0 Troubleshooting Guide
- SupportAssist Enterprise Version 4.0 REST API Guide
- SupportAssist Enterprise Version 4.0 Alert Policy Guide
- SupportAssist Enterprise Version 4.0 Release Notes
- SupportAssist Enterprise Version 4.0 Reportable Items