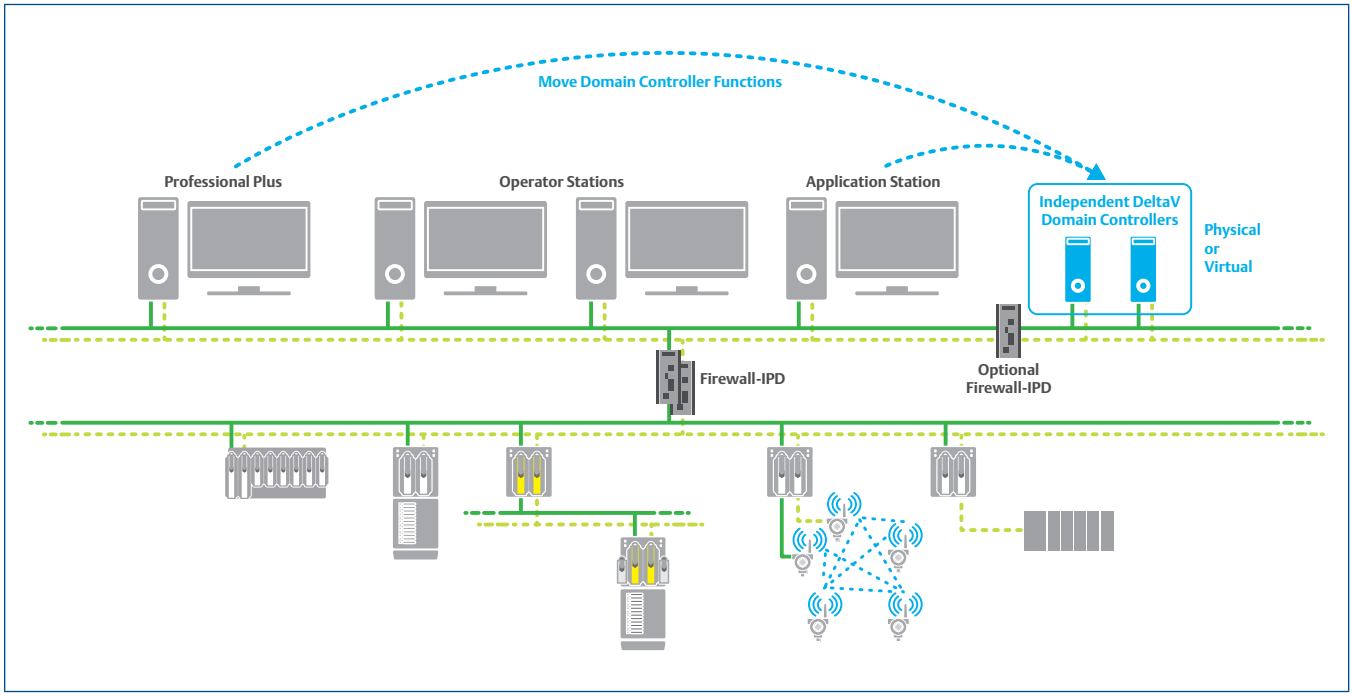
White Paper
September 2022

Independent DeltaV™ Domain Controller

Domain controller functionality can be de-coupled from the Professional Plus / Application stations in DeltaV™ systems version 14.LTS and later.



DELTAV™

EMERSON™

www.emerson.com/deltav

Table of Contents

Introduction

Active Directory was introduced by Microsoft with the release of the Windows 2000 Server Operating System (O/S). DeltaV systems work in conjunction with specific Active Directory features to provide a more secure and manageable production environment. Windows domains provide centralized user accounts and groups, and combined with Windows forests you also get administration, redundancy, and scalability as part of the computers network environment. This whitepaper provides details about the Independent DeltaV Domain Controller (IDDC) functionality introduced in DeltaV version 14.LTS. This whitepaper assumes that you understand the concept of Windows domains and forests.

Starting in DeltaV version 14.LTS, you can de-couple domain controller functionality from the Professional Plus / Application stations with the Independent DeltaV Domain Controller (IDDC). This implementation method enables simpler setup for DeltaV systems in a domain environment. IDDC follows the security guidelines required for industrial control systems as per the emerging ISA/IEC 62443 series of standards with regards to separation of roles and network segmentation.

The domain controller role is very important in Active Directory infrastructure since it holds credentials for all users that are allowed in the domain system. It can also be used by domain administrators to manage security settings on all domain member machines. Without IDDC functionality, the Professional Plus station programmatically becomes the primary domain controller and the Application station can be configured as a backup domain controller. In most systems, Professional Plus and Application stations are also connected to external networks through the L2.5 network connection. And, in most cases, these machines provide Remote Desktop access, OPC communications, etc. which are technically entry points and therefore increase the attack surface to your system by leveraging the domain controllers as an important pivot point.

The next sections in this whitepaper provide more detailed information about how you can implement IDDC functionality in DeltaV version 14.LTS or later.

Note 1: *The Independent DeltaV Domain Controller allows DeltaV domain controllers to be installed on non-DeltaV dependent servers connected to the DeltaV Area Control Network (ACN). This feature is not meant to allow the domain controllers to be installed outside of the DeltaV system environment (i.e., L2.5 network and above), nor to allow DeltaV stations to join a foreign domain (e.g., root automation domain, or enterprise domain). DeltaV systems can be deployed in workgroup and domain environments, and the latter requires local domain controllers running at the DeltaV ACN level and management of the DeltaV users and security settings. Emerson provides limited support (if any) to DeltaV installations that do not follow the recommendations highlighted here.*

Note 2: *Emerson recommends you separate credentials for corporate and control network zones and store credentials in separate trust stores. The Independent DeltaV Domain Controller functionality was not designed to simplify the deployment of single sign-on solutions for multiple control systems that may be somehow connected to the same network infrastructure. Please refer to the whitepapers "Pros and Cons of DeltaV as a Child domain" and "Active Directory Domains and Forests Concept" for more information on this topic.*

Note 3: *An important part of the workstations hardening is only done with Windows Group Policies (GPO) and therefore systems in a workgroup environment will not take advantage of the full hardening aspects provided during DeltaV installation if they are not implemented in a domain environment.*

Feature Description and Use Cases

In DeltaV version 14.LTS, the Independent DeltaV Domain Controller is available if you optionally decide to install the domain controller functionality in different servers than the Professional Plus (as the primary domain controller) or the Application Station (as a backup domain controller).

Domain controllers are not expected to be accessed by all users in a domain environment and they are usually installed on nodes in locations with restricted access, and to a further extent with very few peripherals attached to them. The main goal of this isolation is to prevent credentials from being stolen, or unauthorized access to the domain environment. The main use cases for the Independent DeltaV Domain Controller based on DeltaV system applications are as follows:

- **Domain controller isolation** which is primarily achieved by segmenting DeltaV and domain features during installation. The Independent DeltaV Domain Controller deployment method allows the domain controller to be a dedicated domain controller – no DeltaV user interface applications are required in the server machines used as Independent DeltaV Domain Controllers.
- **Support for Microsoft Credential Guard deployment.** Isolated domain controllers are required on systems that deploy Microsoft's Credential Guard. Microsoft does not recommend enabling the Credential Guard feature in domain controllers.
- **Release the Professional Plus station from running the domain controller role in domain environments.** With the Independent DeltaV Domain Controller implemented, the Professional Plus can be a workstation rather than a server machine and therefore provide high display resolution and multi-monitor support, even in a domain environment. This is true for small systems where the Professional Plus station is not enabled with multiple functionalities beyond the system database. Other requirements will still need server class machine for the Professional Plus station.
- **Simplify upgrades.** De-coupling domain controllers from the DeltaV functions allows for simpler online upgrades that no longer need to deal with transfer of roles or complex steps to maintain the authentication servers up and running.

The Independent DeltaV Domain Controller is an optional deployment, but highly recommended by Emerson to provide added security for DeltaV domain environments, as well as additional DeltaV management flexibility throughout the system lifecycle.

Setting Up the Independent DeltaV Domain Controller

When the Independent DeltaV Domain Controller functionality is implemented, it does not require the server with the domain controller role to run any DeltaV application. Starting in DeltaV version 14.LTS and as part of the DV_Extras folder within the DeltaV installation media, a free-standing installer is available to configure the server machine to be an Independent DeltaV Domain Controller. This installer does not add any DeltaV application to the server machine, but instead, it sets up any server machine running Windows Server 2016 O/S with the expected IP addresses, server hardening, user groups settings, NTP and DNS settings expected to support Active Directory for DeltaV systems. For DeltaV stations the installation and upgrade wizards have been changed to accommodate the Independent DeltaV Domain Controller functionality either on a fresh new install or an upgrade from previous DeltaV versions respectively.

The Independent DeltaV Domain Controller Setup App as well as the DeltaV installation and upgrade wizards strive to deliver an almost fully automated experience – certain steps require user intervention, but they were optimized to reduce the time to be performed. Below you can have an idea of the required steps to add the Independent DeltaV Domain Controller functionality on new systems or during upgrades.

- Installation of the Independent DeltaV Domain Controller on a new DeltaV system:

  1. Run the Independent DeltaV Domain Controller Setup App on the server intended to be the primary domain controller.
  2. Run the Independent DeltaV Domain Controller Setup App on the server intended to be the backup domain controller.
  3. Install DeltaV on the station intended for the Professional Plus function – during installation you will be prompted to choose the Independent DeltaV Domain Controller. The installation steps will automatically make the necessary changes to allow the Professional Plus station to join that domain rather than creating a new one when the Independent DeltaV Domain Controller option is chosen.

> ***Note:*** *the time server function is not transferred to the Independent DeltaV Domain Controller and remains in either the Professional Plus or Application Station as in previous DeltaV releases. Time server settings are still managed within DeltaV even with the Independent DeltaV Domain Controller in place.*

  4. Install DeltaV on the remaining stations per your system architecture (no change to this step compared to previous DeltaV releases).

- Installation of the Independent DeltaV Domain Controller during an upgrade (See next bullet for upgrades from DeltaV version 14.LTS to 14.FP1):

  1. Run Run the Independent DeltaV Domain Controller Setup App on the server intended to be the primary domain controller function. Since the Professional Plus is already a domain controller in the system, the Independent DeltaV Domain Controller will join the domain as another backup domain controller during the upgrade procedure.
  2. Run the Independent DeltaV Domain Controller Setup App on the server intended to be a backup domain controller. This Independent DeltaV Domain Controller will be another backup domain controller in the system during the upgrade procedure.
  3. Run the DeltaV Upgrade Wizard on the Professional Plus station and follow the upgrade steps. The FSMO roles and DNS server are automatically transferred during the upgrade. The Professional Plus / Application stations will be demoted, and they will join the domain as members (no longer as domain controllers). The upgrade process is partially automated, certain manual steps are still required as documented in Books-Online (DVUpgrade.chm file in the DeltaV media). Note that re-installation of the Windows O/S on Professional Plus or Application Station (when they are domain controllers) is always required on upgrades to systems with Independent DeltaV Domain Controllers.
  4. Run the DeltaV Upgrade Wizard on the remaining stations per your system architecture (no change to this step compared to previous DeltaV releases).
  5. Run the DeltaV Upgrade Wizard on the Application station (if it is a backup domain controller) and follow the upgrade steps. Note that re-installation of the Windows O/S is always required (if the Application Station is a domain controller) when upgrading to a system with Independent DeltaV Domain Controllers.

- Installation of the Independent DeltaV Domain Controller during an upgrade to DeltaV version 14.FP1 from DeltaV version 14.LTS:

  - If DeltaV version 14.LTS is not deployed in a domain environment, then users must change from workgroup to domain before deploying IDDC.

- Upgrades from DeltaV version 14.LTS with Feature Pack 1 installed:
  1. If IDDC is already installed prior to the DeltaV version 14.FP1 upgrade, then:
     - Use version 14.LTS Service Pack 1 to upgrade DeltaV stations (domain members).
     - Use the IDDC Setup App available in the DeltaV version 14.FP1 media to update hardening settings of existing IDDCs.
  2. If IDDC is not installed prior to the DeltaV version 14.FP1 upgrade, then:
     - Use IDDC Setup App available in the DeltaV version 14.FP1 media to create IDDC as backup domain controllers in the version 14.LTS system.
     - Use DeltaV Upgrade Wizard to upgrade the DeltaV stations to version 14.FP1, considering a change to IDDC as primary domain controller. The upgrade will automatically demote the Professional Plus and Application Stations which will be changed to domain members
- Upgrades from DeltaV version 14.3 without Feature Pack 1 installed:
  1. If IDDC is already installed prior to the DeltaV version 14.FP1 upgrade, then:
     - Use DeltaV Upgrade Wizard to upgrade the DeltaV stations to version 14.FP1.
     - Use the IDDC Setup App available in the DeltaV version 14.FP1 media to update hardening settings of existing IDDCs.
  2. If IDDC is not installed prior to the DeltaV version 14.FP1 upgrade, then:
     - Use IDDC Setup App available in the DeltaV version 14.FP1 media to create IDDC as backup domain controllers in the version 14.LTS system.
     - Use DeltaV Upgrade Wizard to upgrade the DeltaV stations to version 14.FP1, considering a change to IDDC as primary domain controller. The upgrade will automatically demote the Professional Plus and Application Stations which will be changed to domain members.

Note 1: *Windows O/S re-installation is always required on Professional Plus and Application Stations*
(If they are domain controllers) when upgrading to a system with Independent DeltaV Domain Controllers, even if the starting point is Windows Server 2016 (e.g., upgrades from DeltaV version 13.3.1 to version 14.3 with Independent DeltaV Domain Controller).

Note 2: *The domain controller functional level in DeltaV version 14.3 is set to Windows Server 2016, but during upgrades it remains in Windows Server 2008 to allow different O/S to co-exist in the same domain environment. Manually elevate the domain controller functional level to Windows Server 2016 once all stations have been upgraded to DeltaV version 14.3.*

Note 3: *If you are upgrading from a system with Independent DeltaV Domain Controllers already deployed, you will run the Independent DeltaV Domain Controller Setup App on each of the existing domain controllers to update their security hardening schemes to match the rest of the system. Re-running the Setup App on a domain controller will not force creation or joining of an Active Directory Forest, but instead will simply update hardening on the target domain controller.*

The main goal for the Independent DeltaV Domain Controller functionality is to isolate the domain controller role from other control system functions and make sure domain controllers are not broadly accessible – only domain administrators should have access to the domain controllers in each system.

If your Independent DeltaV Domain Controllers are connected to the L2.5 network, Emerson highly recommends you enable Windows Firewall for the L2.5-related network cards and set it up to allow Active Directory communications only. Emerson is also offering another optional component to further segment the domain controllers' functionality within their own security zone. The DeltaV Controller Firewall-IPD can be re-purposed with a simple configuration change and be installed within the DeltaV ACN and only allow Active Directory communications between the DeltaV system and the Independent DeltaV Domain Controllers. Figure 1 below shows how the network layout would look with DeltaV Controller Firewall-IPDs used to filter Active Directory communications in a DeltaV system (DeltaV Smart Switches omitted in the figure for simplicity).

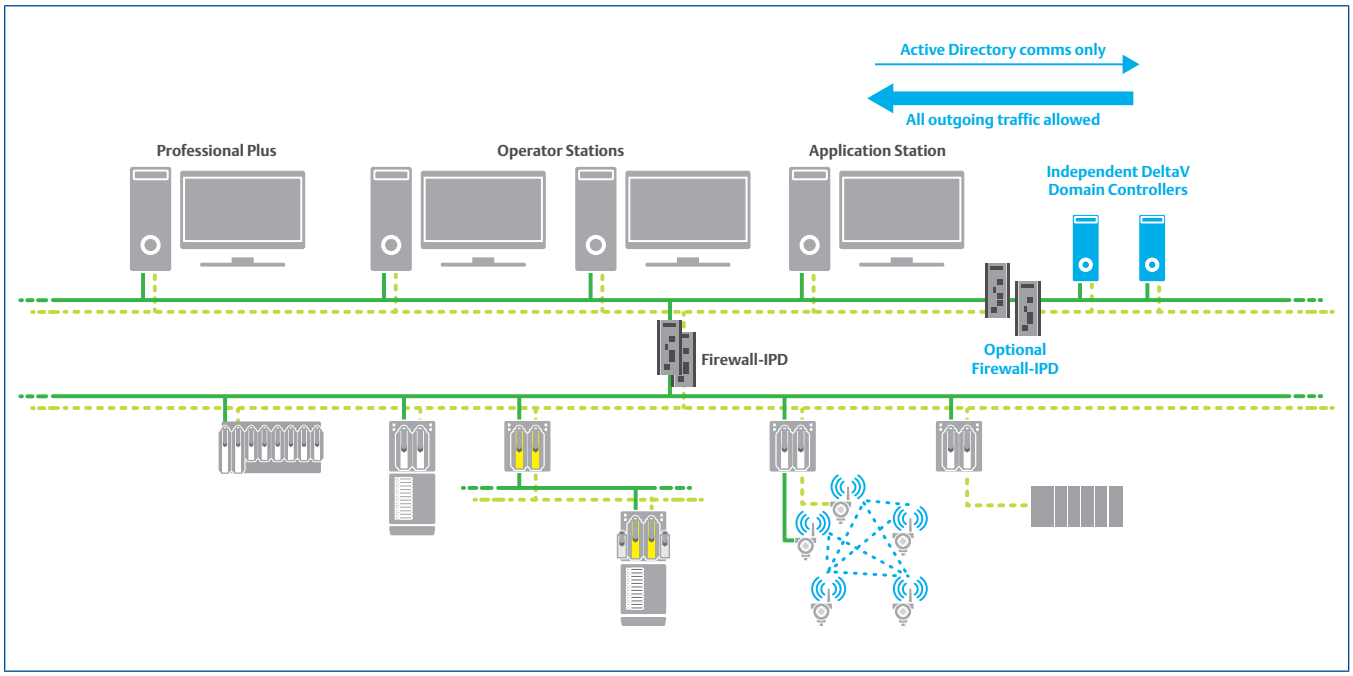


Figure 1 – DeltaV system with Independent DeltaV Domain Controllers and the Firewall-IPD.

Changing the DeltaV Controller Firewall-IPD's configuration is very simple, and a pre-configured template is available for download from the Guardian Support Portal and it can be uploaded to an existing, or newly purchased, DeltaV Controller Firewall-IPD. The new rules set only allows Active Directory communications to pass. Please refer to the Guardian Support Portal to access the Knowledge Base Article for the re-purposing steps.

Below is a list of functions, communication ports, protocols and directions provided by Microsoft that are used by domain controllers and domain members:

Function	Communication Ports	Protocols	Direction
Domain controller to domain controller (RPC) Client to domain controller (RPC)	135	UDP	Incoming / Outgoing
	135	TCP	
Client queries to domain controller (LDAP)	389	UDP	Incoming / Outgoing
	389	TCP	
Kerberos Password Change	464	UDP	Incoming / Outgoing
	464	TCP	
DNS client to domain controller DNS domain controller to domain controller	53	UDP	Incoming / Outgoing
	53	TCP	
Kerberos	88	UDP	Incoming / Outgoing
	88	TCP	
Kerberos V5	464	UDP	Incoming / Outgoing
	464	TCP	
User and Computer Authentication	137	UDP	Incoming / Outgoing
	139	TCP	
File Replication Service Sysvol Share (SMB)	445	UDP	Incoming / Outgoing
	445	TCP	
Global Catalog from Client to domain controller	3268, 3269	TCP	Incoming / Outgoing
Remote Desktop Domain controller Locator	389	UDP	Incoming / Outgoing
	389	TCP	
NTP	123	UDP	Incoming / Outgoing
Group Policy	any	ICMP	Incoming / Outgoing
High Port Range (Ephemeral Ports)	49152 to 65535	TCP	Incoming / Outgoing
Domain controller Certificates (SSL)	636	TCP	Incoming / Outgoing

Table 1 – Communication ports to consider for domain controllers' communication filtering in the network[1]

[1] *"Please refer to the Active Directory and Active Directory domain Services Port Requirements" article from Microsoft for up-to-date information on this topic.*

Access to the Independent DeltaV Domain Controller

On DeltaV version 13.3.1 or prior, you would need to manipulate many settings within DeltaV User Manager to split the administrative functions of a domain vs DeltaV. A direct benefit of the Independent DeltaV Domain Controller is the segregation of roles for users that manage Active Directory on a DeltaV system. For DeltaV version 14.LTS and later, the DeltaV User Manager has a new nomenclature for the 'Windows Administrator' option which is now called 'Local Administrator'.

Local administrators are Windows administrative accounts with full-access permissions on a given machine within the DeltaV network. The local administrator account type does not have domain administrative rights, instead it only has administrative rights on the workstation or server where it is configured using DeltaV User Manager. Local administrators do not have access to the domain controllers necessarily.

Domain administrators are Windows administrative accounts with full-access permissions in the DeltaV domain environment including access to all workstations, servers, and the domain controllers. These account types are created in the domain controller using Windows user management tools only.

The out-of-the-box user's experience changes with the Independent DeltaV Domain Controller based on the segregation of roles. Since DeltaV systems use very limited Active Directory functionality, the changes related to user accounts management are minimal and they are summarized in Table 2.

Account Management Function	Releases prior to DeltaV version 14.LTS	DeltaV version 14.LTS and later
Create or delete a user account OR Change Windows-related privileges (groups, administrative settings, etc.)	Users with Windows administrator privileges have both domain and local administrative privileges and therefore can launch DeltaV User Manager and create/delete user accounts. These operations can be done from any DeltaV station.	Only users with domain administrator privileges can create/delete user accounts in the DeltaV system. Local administrators can only make changes to local accounts existing in the workstation/server (not domain accounts). These operations can be done from any DeltaV station and in the Independent DeltaV Domain Controllers – local access to user accounts on domain controllers requires the use of the built-in Active Directory Users and Computers Windows tool.
Change DeltaV-related privileges (keys, locks, areas, etc.)	Both Windows administrator and DeltaV administrator privileges are required – even to launch DeltaV User Manager.	Users with administrative privileges (Windows or DeltaV) can launch the DeltaV User Manager, but if the DeltaV Administrator privilege is not given to a user, he/she will not be able to configure DeltaV keys and locks to an existing user account – not even his/hers (options are greyed out in DeltaV User Manager).

Table 2 – User's experience changes with the Independent DeltaV domain controller.

Ideally, the Independent DeltaV Domain Controllers will be connected to the DeltaV ACN only, meaning that any additional network cards in the IDDCs are not connected to the L2.5 network - achieving Emerson's recommended network segmentation and domain controllers' isolation. However, there are cases where the domain controllers may need to be connected to the L2.5 network to enable domain authentication schemes that traverse the system boundary. Integration of OPC data, PI Historian, AMS Device Manager among others may require forest trusts if both the L2 and L3/DMZ networks are deployed in a domain environment. In those cases, the recommendation is to enable the Windows Firewall and set it up to match the Emerson Smart Firewall's configuration to allow communications only to the domain controllers that are strictly necessary for Active Directory functions. This recommendation implements isolation through logical network segmentation instead of physical separation.

Figure 2 is an example of this specific use case where complementary products and layered applications are running on a different domain from DeltaV and a forest trust is required.

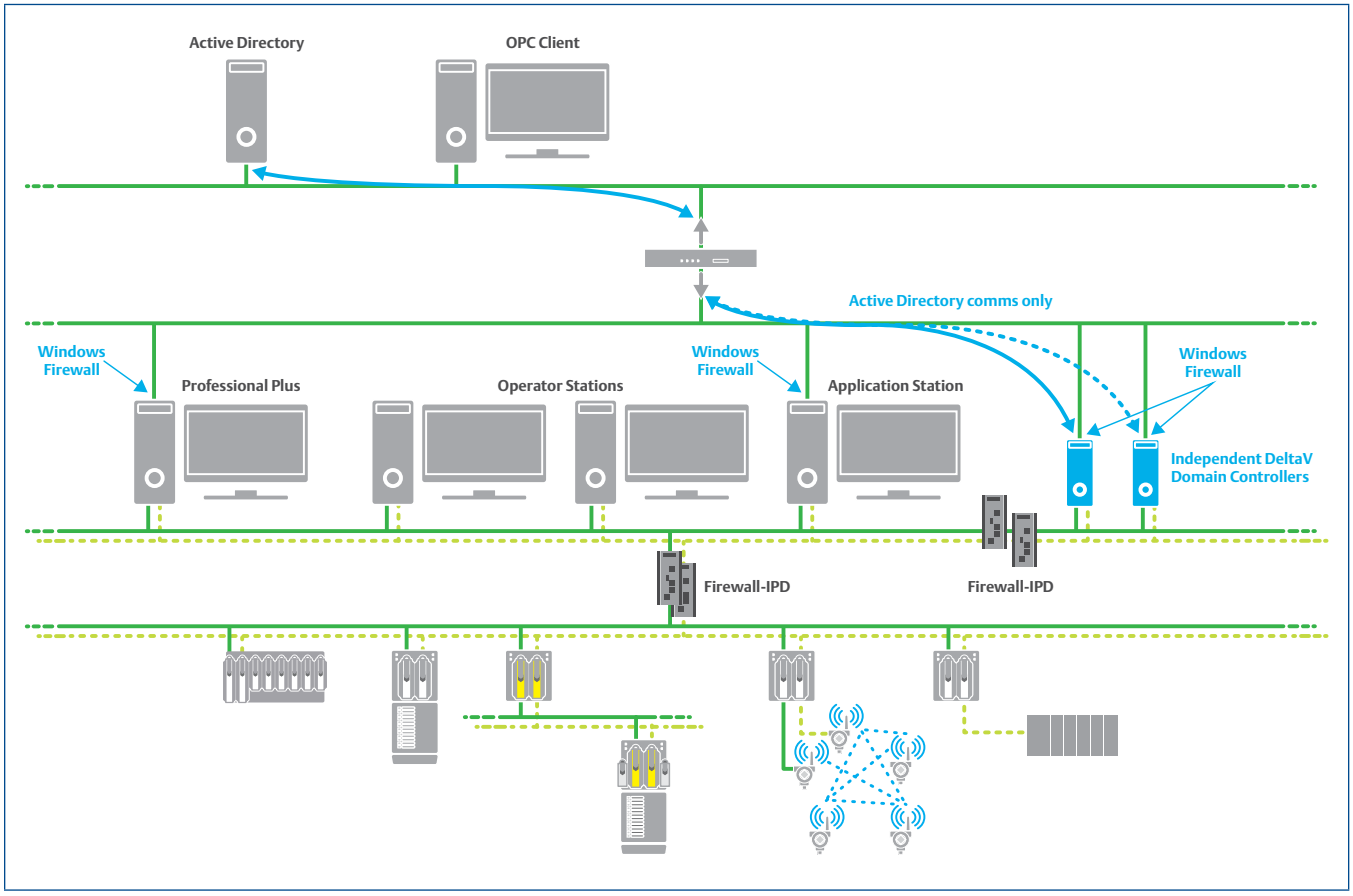


Figure 2 – Forest trust with Independent DeltaV Domain Controllers for complementary products integration into DeltaV.

Correlation with Microsoft Credential Guard

Microsoft Credential Guard is an O/S feature introduced in Windows 10 and Windows Server 2016 O/S by Microsoft that protects computer systems running Windows from a cyber-attack called “pass-the-hash”. This cyber-attack targets the system hashes and allows an attacker to compromise the system using valid/stolen credentials – please refer to the white paper Credential Guard and Device Guard for DeltaV Systems for additional information.

To implement these features, Microsoft provides a list of software and hardware requirements that must be followed to enable full protection. Per Microsoft, Credential Guard is not supported on domain controllers and therefore they should be protected from unauthorized access within networks, especially when Credential Guard is enabled. With that said, the Independent DeltaV Domain Controller becomes a perfect fit for DeltaV systems deployed with Credential Guard enabled in versions 14.LTS and later.

Emerson highly recommends you implement DeltaV in a domain environment, using Microsoft Credential Guard on your DeltaV workstations and servers, and using redundant Independent DeltaV Domain Controllers. This last recommendation is especially important as with Credential Guard the system credentials caching is also disabled for a full protection of credentials within the Windows environment.

Compatibility and Support

The Independent DeltaV Domain Controller is an optional feature and only available for DeltaV version 14.LTS and later. It is also compatible with the DeltaV Virtual Studio versions that support DeltaV version 14.LTS and later. Please refer to the DeltaV Virtual Studio product guides for additional information.

The Independent DeltaV Domain Controller is an inherent DeltaV feature – optionally implemented – that is fully supported by Emerson. The domain controller function is a Windows Server O/S server role, and the Independent DeltaV Domain Controller implementation does not require a full blown DeltaV Server as it will not be running any DeltaV application on it. As such, Emerson offers low-profile servers recommended for the Independent DeltaV Domain Controller installation.

Emerson offers two server-class machines for the Independent DeltaV Domain Controller function. One option is a **tower server**, and the other is a 1**9” rack-mount server** (as indicated in Figure 3), and both with 16GB RAM, four Ethernet ports and dual power supplies – for complete specification and part number information please refer to the DeltaV Workstation and Server Hardware product data sheet.

Independent DeltaV domain controller
Tower Server

Independent DeltaV domain controller
Rack-Mount Server

Figure 3 – Independent DeltaV Domain Controller hardware options provided by Emerson.

Although provided with a 5-year warranty, the server-class machines offered by Emerson for the Independent DeltaV Domain Controller functionality are based on off-the-shelf Dell products and therefore spares are provided by Dell based on Dell factory lead times.

Conclusion

Emerson highly recommends that you deploy DeltaV systems in a domain environment for management and security reasons. The Independent DeltaV Domain Controller functionality further allows users to protect the domain controllers from external attacks, and it releases the Professional Plus / Application stations from running the domain controller role – allowing better system performance and simplifying upgrades.

The Independent DeltaV Domain Controller is also a perfect fit when you decide to implement Credential Guard on your DeltaV system, and in this specific use case redundant domain controllers are needed since we also instruct you to disable credential caching to fully protect credentials within the Windows environment.

Installation of Independent DeltaV Domain Controller functionality is straight forward and as automated as possible, but you can always contact your local Emerson sales office to get a quote for services to design and implement this functionality in a new system or as part of an upgrade.

This product and/or service is expected to provide an additional layer of protection to your DeltaV system to help avoid certain types of undesired actions. This product and/or service represents only one portion of an overall DeltaV system security solution. Emerson does not warrant that the product and/or service or the use of the product and/or service protects the DeltaV system from cyber-attacks, intrusion attempts, unauthorized access, or other malicious activity ("Cyber Attacks"). Emerson shall not be liable for damages, non-performance, or delay caused by Cyber Attacks. Users are solely and completely responsible for their control system security, practices and processes, and for the proper configuration and use of the security products.

Contact Us
www.emerson.com/contactus