Table of Contents

The DataNow Appliance ................................................................................................................................. 6
Appliance Prerequisites .................................................................................................................................. 7
  The Appliance in an Enterprise Network ........................................................................................................ 7
  Supported operating systems and technologies ............................................................................................. 8
  LDAP Directory Service ................................................................................................................................. 8
  DNS Settings .................................................................................................................................................. 8
  Checklist of Required Information ................................................................................................................ 9
Install and Start the DataNow Appliance ........................................................................................................ 10
  Examples ....................................................................................................................................................... 10
  Start the appliance and change your password ............................................................................................ 11
Configure the Appliance Network Identity .................................................................................................... 13
Configure the DataNow Appliance .................................................................................................................. 14
Connect to the Admin Console ........................................................................................................................ 15
Licensing ......................................................................................................................................................... 16
  Upload a License File ..................................................................................................................................... 16
Enable HTTP access ......................................................................................................................................... 17
Configure DNS for file server location .............................................................................................................. 18
Configure the Active Directory Connection ..................................................................................................... 19
Create DataNow Admin users .......................................................................................................................... 21
Check the Appliance Status ............................................................................................................................. 22
Reboot the Appliance ....................................................................................................................................... 23
Configure Certificates for the DataNow Appliance ........................................................................................ 24
Upload an Existing PKCS #12 / PFX Certificate ............................................................................................. 25
Request and apply a certificate using the DataNow appliance ......................................................................... 26
  Create a CSR from the DataNow appliance .................................................................................................... 27
  Request a certificate for your appliance ......................................................................................................... 29
  Apply a certificate to the appliance .................................................................................................................. 32
  Back Up a PKCS #12 / PFX certificate ........................................................................................................... 35
DataNow SMB3 Encryption ............................................................................................................................... 36
  About DataNow SMB3 Encryption .................................................................................................................. 36
  Prerequisites for Kerberos Authentication ....................................................................................................... 37
  Configure Kerberos in the DataNow Admin Console ..................................................................................... 38
Map Point Configuration ................................................................................................................................... 41
Link Based Sharing ......................................................................................................................................... 43
  Set Up the SMTP Server ................................................................................................................................. 44
Create Staging Map Points ............................................................................................................................... 45
General Certificate

SAN Certificates in the DataNow Appliance
The DataNow Appliance

The DataNow virtual appliance is a data broker that forms a connection from your existing file store, through the enterprise firewall, to DataNow clients on end-user workstations and mobile devices. After configuration, the broker allows the DataNow client application to make encrypted connections over public networks or the Internet to files inside the organization.

The appliance connects to an Active Directory using Lightweight Directory Access Protocol (LDAP) and reads the location of home folders for all users. When a user connects a DataNow client to the appliance, it provides a channel to securely synchronize the user’s network home folder to their device.

The appliance is simple to configure and can easily be backed up so it can be recreated quickly. Configure Map Points and define related policies using the appliance to manage behavior for specific organizational units, users and groups of users.
Appliance Prerequisites

The Appliance in an Enterprise Network

We recommend that you install the DataNow appliance on a hypervisor or virtual machine server in the enterprise demilitarized zone (DMZ). From there the appliance:

- Provides secure communications using Secure Socket Layer (SSL) encryption.
- Uses your existing Lightweight Directory Access Protocol (LDAP) to communicate with the Active Directory and configure users, groups and home folders.
- Looks up the location of the file servers using a Domain Name System (DNS) server
- Connects to existing file storage using Server Message Block (SMB) protocol (also known as Common Internet File System, CIFS)

**Note**
DataNow is not compatible with NetApp ONTAP 8.3.1.
- Performs device token authentication using Simple Mail Transfer Protocol (SMTP).

External firewall requirements

For the external firewall, configure the following IP ports:

- **TCP 443** - Clients connect to the DataNow appliance on SSL on port 443 so that they can synchronize files. We recommend that you make this the only external port mapped to the appliance.

Internal firewall requirements

For the internal firewall, configure the following IP ports:

- **TCP 25** - For SMTP to the internal email system.
- **TCP 389** - Active Directory service LDAP on TCP 389.
- **TCP 445** - File store SMB/CIFS on TCP 445.
- **TCP 443** - For internal client connections.
- **TCP 8443** - The web administration interface is available over SSL on http port 8443.
- **TCP 80** - May be required if connecting to internal non-SSL WebDAV resources.
- **UDP 53** - Domain Name System (DNS) on UDP 53.
Additional Ports

The following ports can be enabled if required:

- **UDP 137** - If you enable Windows Internet Name Service (WINS) configuration at the appliance because your infrastructure is dependent upon it, you must open UDP 137 from the DataNow appliance to the configured WINS servers.
- **TCP 8000** - Open this port if you require the AppSense Support service.
- **TCP 8001** - Open this port if you require the Network Load Balancing health check.
- **TCP/UDP 88** - If the DataNow server is secured in a DMZ, you must open port 88 on the firewall for Kerberos Authentication to work.

Supported operating systems and technologies

For details of supported operating systems see the Maintained Platforms Matrix on AppSense Support.

LDAP Directory Service

The appliance needs read-only access to a Microsoft Active Directory (AD) service through a read-only user account.

You can change the home folder field that the appliance uses in the AD records. By default, it uses `homeDirectory`. If you want to use the RDP or Terminal Services home folder then you can specify `CtxWfHomeDir` instead. The home folder feature can be disabled if required.

DNS Settings

DataNow requires internal DNS settings and a public DNS record.

To synchronize user home folders the appliance needs to correctly resolve the address of the file servers where the folders are stored. The appliance uses DNS resolution to locate the correct file server. The appliance DNS settings must specify the DNS servers within the Active Directory and, in order to resolve the short-form file-server addresses used in user AD records, the domain names it should search.

To access the DataNow service on the Internet, you must set up a public DNS record using the DataNow server name. You can then use this public DNS name to generate the Certificate Signing Request (CSR) and apply for a publicly trusted SSL certificate.

A Reverse DNS (PTR) record is required in DNS for each file server that will be accessed by DataNow. This can be validated from a Windows endpoint by typing `ping -a 10.0.0.1` (where 10.0.0.1 is the file server IP v4 address). If reverse DNS is properly configured, it should return the FQDN, for example. server.mycompany.com. If it returns just the IP address, or the single-label host name, for example, server, then it is likely that reverse DNS is not configured correctly.

**Note**

Any changes to DNS configuration may require a reboot of the DataNow appliance to expedite the changes to its DNS cache.
**Checklist of Required Information**

To complete the installation and configuration of the DataNow appliance you need the following information.

<table>
<thead>
<tr>
<th>Hypervisor</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>Hyper-V or VMware ESX</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DataNow Network</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataNow Appliance Name</td>
<td>&lt;appliance name&gt;</td>
</tr>
<tr>
<td>Appliance IP address</td>
<td>&lt;IP address&gt;</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>&lt;IP mask&gt;</td>
</tr>
<tr>
<td>Gateway</td>
<td>&lt;gateway IP&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS servers</td>
<td>&lt;IP addresses&gt;</td>
</tr>
<tr>
<td>DNS search domains</td>
<td>&lt;domain names&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active Directory</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain controllers</td>
<td>&lt;IP addresses&gt;</td>
</tr>
<tr>
<td>LDAP port</td>
<td>&lt;port number&gt; (default 389)</td>
</tr>
<tr>
<td>LDAP bind account</td>
<td><a href="mailto:userID@domain.com">userID@domain.com</a></td>
</tr>
<tr>
<td>LDAP bind password</td>
<td>&lt;password&gt;</td>
</tr>
</tbody>
</table>
Install and Start the DataNow Appliance

1. Log into AppSense Support and download the required DataNow appliance software. Appliance software is available for ESXi VMWARE, Hyper-V 2012 R2 and 2008 R2, and XenServer.
2. Extract the appliance image files and template.
3. In the hypervisor or virtual machine manager, import the template.
4. The template creates the required appliance environment.
5. Start the appliance.

Examples

Install the Appliance on Microsoft Hyper-V

1. Log in to a Windows Server desktop.
2. Download and extract the DataNow Hyper-V zip file to a suitable storage location. Hyper-V uses the virtual hard disks from the location you choose.
3. Start Microsoft Hyper-V Manager.
4. Select the Import Virtual Machine action.
   
   Note
   If you are using System Center, select New Virtual Machine to import the template.
5. Browse to the folder that you extracted. The Import Virtual Machine wizard requires the folder that contains the config.xml file.
6. Select the option to copy the virtual machine and create a new unique ID.
7. Click Import.

Install the Appliance on ESX using vSphere Client

When deploying to ESX, the OVT template defaults networking to “Host Only” and must be manually assigned the correct network before using the appliance.

1. Download and extract the DataNow ESX zip on your local machine.
2. Start the VMware vSphere Client and log in to the host of vCenter Server.
3. From the menu, select File > Deploy OVF Template and follow the wizard.
Start the appliance and change your password

When deploying the appliance, connectivity can be lost when the appliance is migrated to another node, for example, following a reboot. Network configurations will not be applied as dynamic MAC addresses assigned in Hyper-V are lost when the node is moved. To solve this issue, configure a static MAC address in Hyper-V. This must be completed prior to booting the appliance for the first time.

For further information, see Microsoft KB 976724.

1. Start or power on the virtual machine and wait for the appliance to boot.
2. If required, change the input locale. Press F9 to cycle through the available options. This sets the character mapping for your keyboard.

   ![Input Locale Menu](image)

   The default locale for keyboard mapping is US English. If you set a password which contains characters with different mapping in your locale, it could affect your login. For example, if your password is set to P@ssword through the console using a UK English keyboard, it will be recorded as P"ssword Therefore, if you log in from the web client or an SSH client which supports character translation, the wrong password will be supplied and login will fail.

4. Enter the default password: AppSense

   The Main Menu displays.

   **Note**
   The password must be changed before networking can be configured.
   **Do not forget the appliance password. It cannot be recovered or reset.**

5. Select Change Password and press Enter. The password prompt displays.

6. Type the default password, AppSense, and press Enter.
7 Type the new password and press **Enter**.

8 Type the new password again to verify it and press **Enter**.

The Main Menu displays with the Configure networking option now available.
Configure the Appliance Network Identity

1. After the appliance has booted, click in the console and press **F2**. The Password prompt displays.
2. Type the password and press **Enter**. The main menu displays.
3. Use the arrow keys to select **Configure networking** and press **Enter**.

![Main Menu](image)

The Configure networking box displays.

![Configure networking](image)

4. Enter a host name. When you set a host name, the appliance uses it to generate a temporary self-signed SSL certificate.
5. Enter an IP address, subnet mask and a default gateway. The default gateway is the IP address of the internal gateway to services that include, for example, the DNS server, the Active Directory service, the email server and the file store.
6. Press **F10** to save the network settings.
7. From the main menu, select Reboot and press **Enter**. The server reboots then displays the host name and IP address.
Configure the DataNow Appliance

The following processes should be completed in order:

1. Connect to the Admin Console
2. Licensing
3. Enable HTTP access
4. Configure DNS for file server location
5. Configure the Active Directory connection
6. Create DataNow Admin users
7. Check the Appliance Status
8. Reboot the Appliance
9. Configure Certificates for the DataNow Appliance
Connect to the Admin Console

By default, the DataNow Admin Console listens for secure socket layer (SSL) connections on TCP port 8443.

Initially you can use the unqualified server name or IP address. If you want to use the server name you can add the server to your enterprise DNS or add the IP address and server name to the hosts file on your local computer.

1. In a web browser, connect to the DataNow Admin Console by typing https://<server>:8443 in the address bar and pressing Enter.

   Where <server> represents the fully qualified domain name (FQDN) of the DataNow appliance. For example, datanow.appsense.com

   **Note**
   When you configure the appliance network settings, a temporary, self-signed, SSL certificate is generated that uses the unqualified server name specified. Your web browser will indicate that there is a problem with the website’s security certificate because it is self-signed and not issued by a trusted certification authority (CA). You can trust this temporary certificate initially and continue to the website.
   
   Replace this certificate with a trusted certificate containing the server’s fully qualified name.

   The browser connects to the DataNow Admin Console and displays the login screen.

2. Log in to the console:
   - Username: *appliance*
   - Password: The password you configured when you started the appliance.

   **Note**
   By default MS Internet Explorer 9 connects in compatibility mode for intranet sites, that is, sites that do not use the FQDN. You must view the Admin Console with IE9 compatibility view disabled. Press F12 to change the Browser Mode.
Licensing

Before you can set-up and configure your appliance, you must upload a valid license file. License files are provided by AppSense - if you have not received yours, contact AppSense Support. Until the license has been uploaded, the Configuration and Policy tabs are not accessible. When you view your license details, the license status is License Expired.

Upload a License File

1. Select Home > License. If this is the first time you have accessed the appliance or your current license is not valid, the License Status shows License Expired.

2. Click Choose file, navigate to your license file and click Upload License File.

If your license is valid, the license status is updated and details about your license are displayed.

License Status:

License Installed

Appsense Ltd - UK - Daresbury

Licensee Name: Appsense Ltd - UK - Daresbury
License ID: 36296543-d2e5-4f5e-8e7-3e8908b39d21
License Type: Evaluation
Expires: Wed Dec 07 2016 00:00:00 GMT+0000 (GMT Standard Time)
Date Issued: Tue Dec 08 2015 09:22:12 GMT+0000 (GMT Standard Time)

Features Included:

DataNow Enterprise (F5E79D27-B94C-4DF1-9968-58DE8FCAFF74)  Appliance, 1 Users versions: 3.*** - 3.***

Once installed, you can access all areas of the appliance enabling you to configure DataNow.
Enable HTTP access

Select **Configuration > Advanced.**

In the HTTP Access area of the Advanced options, configure the required setting and click **Update** to apply.

**Caution**

This option should only be used to enable connection by HTTP in a load balanced environment or with an SSL offload appliance.

![HTTP Access settings](image)
Configure DNS for file server location

To synchronize user home folders the appliance needs to correctly address the file servers where the folders are stored. The appliance uses DNS to resolve the file server IP address.

The appliance DNS settings must specify the DNS servers within the Active Directory (AD) and the domain names it should search in order to resolve the short-form file-server addresses used in user AD records.

1. Select **Configuration > DNS** and click **Edit**.
2. Complete the following DNS Settings:
   - DNS Server IP address.
   - DNS Search Domain.
   - WINS Server - WINS Server settings are optional and should only be added if an AD server uses WINS for homeDirectory settings.
     To add further DNS server details, use the + buttons.
3. Click **Save** to commit your DNS settings.
Configure the Active Directory Connection

The appliance needs read-only access to a Microsoft Active Directory (AD) service through a read-only user account. The appliance communicates with the Active Directory using Lightweight Directory Access Protocol (LDAP). The LDAP port is configurable - the default is port 389.

**Note**
To use a name for the directory server you must set the DNS IP address and search domains first.

1. Select **Configuration** > **Active Directory** and click **Add New**.

2. Complete the following Active Directory settings:
   - **Name** - A descriptive name for the server. This is a free text field used to easily identify servers.
   - **Server** - The name or IP address of the LDAP server.
   - **Port** - The port for your AD. The default for LDAP communication is 389.
   - **Home Directory Field** - Select which field to use for active directory. The default setting is homeDirectory but this can be changed to use a different AD attribute or disabled if required.
   - **Bind User** - A username with read permissions to the required records. This user account is used by the appliance to synchronize with the directory. Format - username@domain or domain\user.
   - **Bind Password** - The password for the bind user.
   - **Enable SSL** - Adds further encryption between the DataNow and LDAP servers. When this option is applied, the port setting is automatically updated to use port 636.

3. Click **Save** to commit your Active Directory settings.

4. Reboot the appliance.
5 Following the appliance restart, select **Home > Status** to verify that the WebServer, Appliance Services, DataNow Server and Active Directory have been configured.
Create DataNow Admin users

After connecting the Active Directory, to continue configuring the appliance, it is recommended that you create a DataNow admin user in the console. DataNow admin users log in to the console using their domain credentials and can synchronize DataNow users with the Active Directory without rebooting the appliance. This is an optional process for delegated admins, as all appliance actions can be performed using the appliance login.

1. Select **Configuration > Admin Users** and click **Add User**. The Admin Users search field is displayed.

2. Enter a username or part of the username you want to add.

3. If required, click **Browse** to target a specific domain.

4. Click **Search**. Any users matching the search criteria are displayed.

5. Select a user and click **OK**.

   If you are configuring the appliance for the first time, you must log out as the appliance user and log in again as an admin user before continuing.

6. Click **Log out**.

7. Log in as the admin user. The username format is domain\username. The UPN style login is also supported, for example, username@domain.
Check the Appliance Status

Following a reboot, the Status page is automatically displayed. This shows you the areas of the appliance which are configured and those areas requiring attention. Select **Home > Status** to view the Appliance status.

![Appliance Status Check](image.png)

- **OK** Web Server
- **OK** Appliance Services
- **OK** DataNow Server
- **OK** Active Directory

**Notifications:**
- **⚠️** This server's license will expire in 50 days. Please upload a new license file to ensure no interruption of service.
- **⚠️** Please generate a CSR and upload a valid SSL certificate. [Set SSL Certificate](#)

**Download Appliance Log and Configuration report bundle**

**Reboot**
- Rebooting the server will cause the DataNow service to be unavailable for a few minutes.
Reboot the Appliance

When configuring the appliance or updating its settings, a reboot is required for the settings to take effect.

To reboot, select **Home > Status** and click **Reboot**.
Configure Certificates for the DataNow Appliance

If you have an existing certificate - Upload an Existing PKCS #12 / PFX Certificate

If you need to request a new certificate from a Certification Authority - Request and Apply a Certificate Using the Admin Console
Upload an Existing PKCS #12 / PFX Certificate

To use an existing certificate for DataNow, it must fulfill the following criteria:

- The certificate’s CN must match the URL for DataNow (unless a wildcard is used)
- The certificate must be valid for the server authority
- The private key must be available to export in PFX/P12
- The certificate must contain the full chain
- The certificate must have a valid date

If your certificate conforms to all of the above, it can be uploaded to the appliance.

1. Select Configuration > SSL Certificate.
2. In the If you have an existing certificate you’d like to use area, click Choose File.
3. Browse to the location of your certificate.
4. If the certificate was created with an encryption password, type it into the field provided.
5. Click Upload Certificate.
Request and apply a certificate using the DataNow appliance

The DataNow Admin Console allows to create a Certificate Signing Request (CSR) for your appliance. Once the CSR is generated, a trusted person within your organization can apply for a public certificate from one of the public Certification Authorities (CA). A trusted person is normally a director or someone publicly acknowledged to represent the organization. The process is split into four sections:

- Create a CSR from the DataNow Appliance
- Request a certificate for your appliance
- Prepare your certificates
- Apply a certificate to the DataNow appliance
Create a CSR from the DataNow appliance

1. Select **Configuration > SSL Certificate**.

2. Expand the **To obtain a certificate from a Certificate Authority** section and complete the following fields:

   - **Host Name** - The fully-qualified domain name of the server where the certificate will be installed. Wildcard domains can be specified with a * prefix. The host name does not have to match the appliance host name set in the appliance console. However, the host name you provide must match the FQDN on your DNS ‘A’ records. For further information about wildcards and SAN attributed certificates, see [DataNow SAN Certificates](#).

   - **Company/Organization Name** - The name of the organization requesting the certificate.

   - **Organizational Unit** - The division within the organization. For example, Engineering or Human Resources, or if applicable, the database administrator name for the organization.

   - **City** - The full name of the city where the organization is located. Do not use codes or abbreviations.

   - **State/Province** - The full name of the state or province where the organization is located. Do not use abbreviations or codes.

   - **Country** - The two digit ISO country code where the organization is located. For example, US, FR.

   - **Email** - The email address that will be a point of contact for the certificate request.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>DN.DemoLab.com</td>
<td>The fully-qualified domain name of the server where the certificate will be installed. Wildcard domains can be specified using a * prefix.</td>
</tr>
<tr>
<td>Company/Organization Name</td>
<td>Demolab</td>
<td>The name of the company or organization requesting the certificate.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>IT</td>
<td>The division within an organization, such as &quot;Engineering&quot; or &quot;Human Resources&quot;, or if applicable, the DBA (doing business as) name of the organization.</td>
</tr>
<tr>
<td>City</td>
<td>Warrington</td>
<td>The full name of the City where the company/organization is located.</td>
</tr>
<tr>
<td>State/Province</td>
<td>Cheshire</td>
<td>The full name of the State/Province where the company/organization is located (do not use codes/abbreviations).</td>
</tr>
<tr>
<td>Country</td>
<td>UK</td>
<td>The 2-digit ISO Country Code of the country where the company/organization is located.</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:admin@demolab.com">admin@demolab.com</a></td>
<td>The email address that will act as a point of contact for this certificate request.</td>
</tr>
</tbody>
</table>

[Create CSR](#)
3 Click **Create CSR**.

A text box displays the certificate request data.

```
To obtain a certificate request:

---BEGIN CERTIFICATE REQUEST----
MIICICIjCCAcGwGAoIBAQCMAgCAAwCAYYZAtADCAwggUCAgMEAwIBAgIICwIw
h0IzEEJUtEkAAQgABAAAhqEAcTkiibf0hU1wU21XiGCnAgSIwDQgNgAwIw
CQ undertake to help me the certificate request. A text box displays the certificate request data.

**Note**

Every time you use the Generate New CSR option, the unique server key is changed making any previous certificates, generated for this appliance, invalid.

4 Copy the entire text including the lines containing **BEGIN CERTIFICATE REQUEST** and **END CERTIFICATE REQUEST** and save it as a TXT file.
Request a certificate for your appliance

This section describes how to submit a certificate request using a Public CA.

Request a Certificate Using a Public Certificate Authority

This process uses a Comodo free 90 day certificate as an example - it is subject to change at the discretion of the PCA and your process will vary depending on the PCA you are using.

1. Navigate to http://www.comodo.com
2. Select Free SSL Certificate.
3. Select Free Trial SSL option.
4. Select Free Trial SSL option again.
5. Paste the CSR you generated into the Provide your CSR text box.
7. Define the remaining options as required and click Next.
8. Enter your corporate details and create an account.
9. Submit your request.
   Once the request has been validated you will be sent a confirmation followed by your SSL certificate.
10. Open the certificate. It should include Root, Chain and Standard certificates.
    You can view the certificate types from the View Certificate dialog in the Certification Path tab.

Install a Comodo certificate

Before you apply the Comodo Server standard certificate, you must download a series of intermediate certificates.

1. Navigate to the following URL:
   https://support.comodo.com/index.php?_m=downloads&_a=view&parentcategoryid=20&pcid=1&nav=0,1
2. Download the following certificates:
   - [Intermediate #1] ComodoUTN SGCCA
   - [Intermediate #2] UTNAddTrustSGCCA
   - [Intermediate #3] EssentialSSLCA

All intermediate certificates must be installed on the appliance before the standard certificate provided by Comodo is installed.
Prepare your certificates

Your certificate will be a web certificate and should include intermediate and root certificates. Once installed you can access your DataNow certificate from Certificate Manager. Before you can apply your certificates to the DataNow appliance, they must be exported.

Export certificates

1. Open Certificate Manager.

2. Right click on the root DataNow certificate and select **Open** from the short-cut menu.

3. Select the **Details** tab and click **Copy to File**.

4. The Certificate Export Wizard opens, click **Next**.
5 Select **Base-64 encoded X.509 (.CER)** and click **Next**.

6 Browse to where you want to save the certificate, give the root certificate a name and click **Next**.

7 Review your settings and click **Finish** to start the export.

    You are notified when the certificate has been successfully exported.

8 Repeat this process for your Standard certificate and any Intermediate certificates.
Apply a certificate to the appliance

This section describes how to apply a certificate for both Private and Public Certification Authority (CA). Most major public CA root certificates are included in the DataNow appliance and in client operating systems for the computers and devices that support the DataNow client.

**Note**
You must have the root certificate from your Private CA. If your CA is a subordinate CA you will require its certificate (intermediate/chain) and any other subordinate CA certificates and the root certificate.

DataNow uses 2048-bit RSA certificates in Base64 PEM format which must be installed in the following order:

1. Root Certificate
2. Chain 1 Certificate
3. Chain 2 Certificate
4. Server Certificate

**Note**
Before continuing with this process, we recommend that you take a hypervisor snapshot to back up the pending CSR state prior to any further configuration.
Apply certificates to DataNow

**Tip**
To restart the certificate upload process, click **Reset Certificates**. Any entered data is deleted without removing the pending Certificate Signing Request (CSR).

1. Locate the CER file for the root certificate.
2. Open the certificate in a text editor, such as Notepad.
3. Copy the text including the BEGIN CERTIFICATE and END CERTIFICATE statements.
4. In DataNow Admin Console, select Configuration > SSL Certificate.
5. In the Set New Certificate area of the DataNow appliance, paste the certificate details into the text box.
6. Select **Root Certificate** and click **Upload Certificate**.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICeTCCAXGwAwIBAgICAJAgMCAYGp8 SHA256
+-----END CERTIFICATE REQUEST-----
```

Certificate Type:
- **Root Certificate**
- **Chain Certificate/Bundle**
- **Server Certificate**

![Upload Certificate button]

Reset pending root and chain certificates:

![Reset Certificates button]

A message will confirm that the certificate has been installed.

7. Add your Chain Certificate - select **Chain Certificate/Bundle** and click **Upload Certificate**.

**Caution**
If your chain is a bundle, you must add each chain certificate (e.g. number 3 then number 3) to the text box in reverse order.
In the example below, Chain 2 has been added followed by Chain 1.

A message will confirm that the certificate has been installed.

8 Add your Server Certificate - select **Server Certificate** and click **Upload Certificate**.

When all certificates have successfully installed, an information message informs you that the certificate has been enrolled.

9 Reboot the appliance to apply the certificates to the web service.

To test the certificate, close and reopen the browser and connect to the Admin Console using the fully qualified server name specified in the certificate. If the certificates are installed correctly, the browser connects securely without any security warnings.

**Note**

We recommend that you back up the DataNow appliance configuration snapshot.
Back Up a PKCS #12 / PFX certificate

A PKCS #12 / PFX certificate containing your encrypted SSL certificate and your private keys can be downloaded from your DataNow appliance. You can use this when configuring new installations of the appliance without having to repeat the process of configuring an SSL certificate.

1. Click the Configuration tab and click SSL Certificate.
2. Locate the To back up the existing SSL certificate chain area.

   ▼ To back up the existing SSL certificate chain

   Download the current SSL certificate in PKCS #12 (.p12) format.
   IMPORTANT - Please note the encryption password and save in safe location.
   Set Encryption Password: 
   [Enter]
   Download P12

3. If required, enter an encryption password.
   Encryption passwords are optional and add an extra level of security. If you set a password during download, it must be entered to successfully upload your certificate. Passwords are non-recoverable, so it is important that you remember the password or store it in a safe location.

4. Click Download P12 and save the certificate.
DataNow SMB3 Encryption

About DataNow SMB3 Encryption

DataNow supports SMB3.02 encryption for all traffic from DataNow servers to back end storage. Support is for SMB3.02 encrypted shares using Windows Server 2012 R2 as the reference platform. Using encrypted SMB3.02 shares requires valid Kerberos configuration items in the DataNow server to support authentication. It also requires that map points are specified using hostname rather than IP address. It is preferable to use the Fully Qualified Domain Name although using the Shortname will work if valid DNS search domains have been configured.

**Note**
If the DataNow server is secured in a DMZ then port 88 needs to be open between DataNow and Active Directory on the firewall for this to work. This applies to both TCP and UDP protocols.

Two modes of authentication are available:

- Username and password authentication on the endpoint with the DataNow server switching to Kerberos authentication to communicate securely with the back end SMB3.02 share.

- Using Kerberos from the endpoint right through to the SMB3.02 share utilizing ticket forwarding.

For both authentication modes, reverse IP lookups for file servers and domain controllers must be setup and the clock skew between DataNow and must be less than five minutes.

**Note**
In order for DataNow to function correctly, AES-128 encryption must be enabled on the Key Distribution Center (KDC).
Prerequisites for Kerberos Authentication

**Note**

These prerequisites are only required for configuring Kerberos authentication using ticket forwarding.

In order to utilise Kerberos authentication against the DataNow appliance, Active Directory needs to be configured with a user that allows:

A The Kerberos keytab to be acquired from a user account so the server can trust the authorised user to access it.

B Pre-authentication checks.

C Kerberos Ticket Granting services, which are part of Active Directory, to determine the ‘service principal’ used to access the DataNow appliance and obtain a ticket to establish an authorised connection to the DataNow appliance.

D The re-use of service tickets sent to the platform so that the service can access data upon the user’s behalf (Kerberos Constrained Delegation). This is required if setting up Kerberos on the client.

To perform the setup, complete the following steps:

1 Create a user account within Active Directory for this purpose and set a password that will be used by the appliance to perform actions A and B. It is recommended that this account is not an admin account.

   **Note**

   To ensure the correct default domain is used, the username for this account must include the relevant realm name. The required format is user@realm, for example, bsmith@datanow.local.

2 Set the account so that the password cannot be changed and never expires. This is recommended as it removes the need to reconfigure the platform to use new credentials.

3 Ensure DNS references the DataNow server and always use the full DNS name to access the DataNow server in the future.

4 Take the DNS name and use the `setspn` tool from a domain controller to add HTTP Kerberos service principals that match the DNS name to the user account.

   For example, if the user account is called ‘dnpreauth’ and the DNS name that will be used to access the user account is ‘dn.mycompany.com’, issue the following `setspn` commands on a domain controller and ensure they run error free:

   ```
   setspn -S http/dn.mycompany.com dnpreauth
   ```

   Following step 4 a new ‘Delegation’ tab appears in Active Directory Users and Computers associated with the user account. This tab is used to allow the Kerberos Ticket Granting server within AD to locate the key information associated with the user account and allow a token to be returned to the client system to access the DataNow appliance.

5 Select the Delegation tab for the pre-authenticate user and select **Trust this user for delegation to any service (Kerberos only)**. The DataNow appliance has authorisation to utilise the Kerberos ticket forwarded to it by the DataNow client or web browser so that it can reuse the user identity to access file service resources.
Configure Kerberos in the DataNow Admin Console

This process describes how to configure the DataNow Admin console for Kerberos authentication.

Kerberos Realm

1. In the DataNow Web Admin console, select Configuration > Kerberos.
2. Click Add Realm.
   The Add/Edit Kerberos Realm dialog displays.

   ![Add/Edit Kerberos Realm dialog]

3. In the Domain field, enter the default domain name.
4. Enter the fully qualified domain name of the domain Key Distribution Center (KDC). This is usually the same DNS as the Active Directory controller.

   Tip
   If you are unsure of the KDC name, use `nslookup _kerberos._tcp.<domainFQDN>` from a domain joined client to get the IP of the KDC. The use `ping -a <ip address>` to get the name of the KDC.
5. Click OK.
6 Details of the realm are added to the Kerberos section of the screen. The name of the realm is automatically added. Realm names are case sensitive and are usually the same as the domain name in upper-case letters.

7 Repeat steps 2 to 6 for all relevant realms. This ensures successful authentication to all shares added as map points.

8 Click Save.

Once all configuration is complete, enable SMB3.02 protocol on Server 2012 R2 share otherwise data will not be encrypted in transit.

For further details, see http://blogs.technet.com/b/filecab/archive/2012/05/03/smb-3-security-enhancements-in-windows-server-2012.aspx.
Kerberos Token Size

Set the maximum token size for users in your environment. The default value is 12k and this can be increased up to 64k to accommodate users with large tokens.

- **Kerberos Preauthentication**

This setting is only required when configuring encryption for Kerberos from the client. A Preauth user is not required for username and password authentication.

Select **Configuration > Kerberos**.

In the Kerberos Preauthentication section, enter the username and password for the Preauth user.

**Note**

Only one Preauth user can be added. See the [prerequisites](#) for details about setting up this user.
Map Point Configuration

Map points allow usage policy sets to be targeted to different users based on the server they connect to and their OU membership. You can create Map Points for whole OUs, user groups and individual users to create a usage policy which meets their requirements whilst adhering to your security policy.

There are two parts to setting a Map Point:

- **Connection String** - Define the DataNow server for the Map Point and set the download policy.
- **Policy** - Define usage policies and platform access for the Map Point.

1. Select **Configuration > Map Points** and click **Add New**. Or click **Edit** to update an existing Map Point.

2. Enter a name for your map point. This can be any value to easily identify the map point.
   
   **Caution**
   
   The name "Home" is reserved for use by Active Directory home drive settings and should not be set as the name of a webdav or SMB map point.
   
   Do not name a Map Point "Share".

3. Enter a connection string.
   
   - It is recommended that file servers are entered as fully qualified domain names (FQDN), particularly if you are using Kerberos authentication.
   
   - SMB connection strings must begin with \\
   
   - WebDav connection strings must begin with http:// or https:// To designate a user directory, insert %UserName% into the share path, for example, http://servername.company.com/users/%UserName%). %UserName% is case sensitive.

4. Select the required sync mode:
   
   - **Manual: Only download files as requested by the user** - Files are downloaded to a user devices as they are opened.
   
   - **Automatic: Download/sync all files for this map point** - All DataNow files are downloaded locally when the user logs in to DataNow and changed and new local files are automatically synchronized with the server.

   **Note**
   
   For Windows clients, exclusions can be applied that prevent certain files being automatically downloaded. For example, certain file types or files above a certain size can be prevented from being automatically downloaded. See File Sync Controls.

5. Click **Save**.
To set a policy for the map point, click the **Set policy for this map point.**

<table>
<thead>
<tr>
<th>Temp Area</th>
<th>Set policy for this map point</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name:</strong></td>
<td>Temp Area</td>
</tr>
<tr>
<td><strong>ConnectionString:</strong></td>
<td>\WavPoint\Temp Area</td>
</tr>
<tr>
<td><strong>Sync Mode:</strong></td>
<td>Manual. Only download files as requested by the user.</td>
</tr>
</tbody>
</table>
Link Based Sharing

Link Based Sharing provides DataNow users with a fast and efficient way to share content. Once sharing has been configured in the admin console, it can be enabled for the required map points and the type of receivers that are able to access the files can be defined. DataNow classifies receivers into two groups:

- **Internal** - Any employee of the organization as defined by membership of the company’s Active Directory.
- **External** - Anyone not in the above group.

DataNow saves a version of the shared files and automatically creates links which are emailed to listed recipients. For external receivers, DataNow automatically enrolls them and sends access details to the shared content.

Preparation

Sharing files using DataNow requires the Server Administrator to create dedicated staging areas for the two types of receivers. These dedicated areas can be on any AD joined file server, NAS or SAN.

Steps required for Internal Link Based Sharing

1. Create an SMB share. This can be any name you choose.
2. Provide all domain users with read/write access.

Steps required for External Link Based Sharing

1. Create an SMB share. This can be any name you choose.
2. Provide all domain users with read/write access.
3. Create a new domain user with read only access to the external share.

Admin Console

You must configure SMTP to send the emails containing the links, create new Staging Map Points to hold the shared files, enable sharing on your map points and set the expiration time for the shares before using the Link Based Sharing feature.
Set Up the SMTP Server

Set up SMTP to use the required account for initiating Link Based Sharing emails.

**Caution**
The server URL, provided in the client’s request, is used to create the link included in emails to users. The DataNow server URL configured for your company’s appliances must be accessible externally.

1. Select **Configuration > Advanced**.

2. In the SMTP Configuration section, enter the details of the SMTP server and email address:
   - Hostname or IP address of the SMTP server
   - SMTP server port number
   - Encryption type to use when sending emails
   - The email address to send emails from
   - Email address to receive test email
   - Indicate if authentication is required and, if so, provide the username and password

3. Click **Update**.

```
<table>
<thead>
<tr>
<th>SMTP Server Hostname/IP:</th>
<th>smtp.demolab.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Port:</td>
<td>25</td>
</tr>
<tr>
<td>Encryption Type:</td>
<td>TLS, SSL, None</td>
</tr>
<tr>
<td>From Address:</td>
<td><a href="mailto:administrator@demolab.com">administrator@demolab.com</a></td>
</tr>
<tr>
<td>Send test email to:</td>
<td></td>
</tr>
<tr>
<td>Requires Authentication:</td>
<td>✓</td>
</tr>
<tr>
<td>Username:</td>
<td><a href="mailto:administrator@demolab.com">administrator@demolab.com</a></td>
</tr>
<tr>
<td>Password:</td>
<td>*****************</td>
</tr>
</tbody>
</table>
```

Update
Create Staging Map Points

Set up Staging Map Points to enable files to be shared internally and externally. You can only have two staging map points; one internal and one external.

1. Select Configuration > Staging Areas.
2. Click Add New.
3. Enter details of the Internal Staging Map Point:
   - Name for the staging area
   - Connection string for the staging area
   - Select Internal User Access from the drop-down

   ![Add New Staging Area](image)

4. Click Save.
5. Repeat this process for an External Staging Map Point if you want to enable Link Based Sharing for non-AD users, adding the credentials of the External AD User account you are using to enable the external staging area.

   ![Add New Staging Area](image)

6. Click Save.
Enable Link Based Sharing on Map Points

Enable Link Based Sharing on your map points by editing your Map Point Access Policy.

1. Select **Policy > Map Point Access**.
2. Click **Edit** for the required map point.
3. Select the users for whom you want to enable Sharing. Sharing can be enabled for All Users associated with the map point or create individual policies for selected OUs, user groups and/or individual users.
   
   **Tip**
   Click **Add** for an OU, User Group or Individual User to define a specific policies.

4. Open the appropriate Map Point and set the policy for internal and external users.

   You can apply the following settings for each type:
   
   - **Disabled** - Link based sharing is not available for users connecting to this map point. If link based sharing is disabled for internal users, it cannot be enabled for external users on the same map point.
   - **Read-only** - All shares are read-only for this map point. Users can download files but not upload files to shares.
   - **Collaboration** - Users can download and upload files to shares. Internal users can also delete files they upload whilst external users cannot.

   In the example below, Link Based Sharing has been disabled for external users and for the map point. Internal users have collaborative access to shares.

5. Click **Save** to apply the setting.

6. Repeat these steps for any other Map Points where Link Based Sharing is required.
Set the Automatic Expiration for Link Based Sharing

Set the global expiration for the Link Based Sharing by editing your Global Policy. When a share expires, shared files are removed. If you do not want the Link Based Sharing to have an expiry date, do not enable the Sharing policy.

1. Select **Policy > Global**.

2. Click **Edit**.

3. Set the Sharing policy to **On**.

4. Enter the number of days the shared links will be active for.

   ![Sharing](image)

   **Note**
   
   The figure set here is also the number of days a share is extended by when an expiry date is extended.

5. Click **Save**.
DataNow Version

Check which version of DataNow you are running and upload new patches of the software.

Select **Home > Version**.

The left-hand side of the version view shows the version numbers of the components which make up the appliance.

<table>
<thead>
<tr>
<th>Components</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Configuration Services</td>
<td>release - 3.6.6.8</td>
</tr>
<tr>
<td>Appliance Text Console</td>
<td>release - 3.0.2.1</td>
</tr>
<tr>
<td>Appliance Operating System</td>
<td>release - 20140624</td>
</tr>
<tr>
<td>DataNow Server</td>
<td>release - 3.6.7.14</td>
</tr>
<tr>
<td>DataNow Web Admin</td>
<td>release - 3.6.7.50</td>
</tr>
<tr>
<td>DataNow Web Client</td>
<td>release - 3.6.0.33</td>
</tr>
<tr>
<td>DataNow Appliance Plugins</td>
<td>release - 3.6.6.13</td>
</tr>
</tbody>
</table>
Apply a DataNow Patch

DataNow software can be updated by applying a patch, supplied by AppSense, which can be uploaded through your appliance. If clustering is enabled and a patch server has been set, patches are applied in the Cluster tab.

1. Log into AppSense Support and navigate to the DataNow software page.
2. Click the link for the required software.
3. Log in to the DataNow Appliance.
   - In the Status section, details of the current patch version are displayed.
5. Click Choose File and navigate to a DataNow patch file.
   - The screen updates to list the components that the patch is updating and their version numbers.
   - Click a patch to view further details.
6. Select the required patch and click Deploy Update file.

To complete the patch install, the server automatically reboots. Connected devices are unable to communicate with the server for few minutes whilst the reboot completes.
Backup and Restore

You can back up your appliance configuration information from within the DataNow appliance. The whole personality of the appliance and the SSL certificates are backed up to create a snapshot that can be used to configure one or more appliances with the same settings.

Backup an Appliance Configuration

1. Select **Home > Backup & Restore**.

2. In the Backup Appliance Configuration section of the page, enter an Encryption Password in the field provided. This is an optional level of security which requires the same password to be entered when restoring the configuration.

   **Note**
   If set, it is important that you do not lose or forget an encryption password as they are non-recoverable and the backup will become unusable.

3. In the Backup Appliance Configuration section of the page, click **Download Snapshot**.

   The configuration snapshot is saved to your default download location.

Restore an Appliance Configuration

1. Select **Home > Backup & Restore**.

2. Click **Browse** and locate the required configuration snapshot.

3. If required, enter the encryption password, defined when the snapshot was created. If you did not set a password, leave the field blank.

4. Click **Restore Settings**.

5. Reboot the appliance.

   The settings from the snapshot are applied to the appliance.
Clustering

DataNow supports clustered infrastructures and failover processing and is fully scalable to meet the varying demands of organizations.

If an appliance is taken offline, the DataNow service is maintained by seamlessly switching to another appliance in the cluster. Although users are momentarily disconnected, they are automatically returned to the service without losing their session state. Any transactions which have not been committed to the database are rolled back.

**Note**
When setting up the load balancer, ensure that session persistence is setup for the DataNow cluster. It is recommended that the cookie insert method is used.

**Set up the Initial Cluster Node**

**Prerequisites**

Before configuring clustering:

- Ensure all appliances that will be in your cluster are of the same version.
- Create a new blank database in the default SQL instance (SQL Server 2005, 2008, 2008R2 and 2012 are supported).
- Create a new SQL account. It is recommended that the SQL Service account has DBO privileges.
- Configure the switching environment to allow Broadcast traffic.
- Ensure all cluster nodes that are to share common settings are available on the same network to allow low frequency broadcast discovery between the cluster peers.
- Take a backup of the current appliance configuration.

**Enable Clustering on the First DataNow Appliance**

1. Boot up the appliance for the first cluster node.
2. Press **F2** and logon.
3. Select **Cluster Configuration** and press **Enter**.
4. Enter a cluster name.
5. Enter a port number. The default port is 49152 but you can use any port from 49152 to 65535.
6. Press **F10** to save the cluster configuration.

**Tip**
To disable clustering, use the process above, leaving the Cluster Name field blank.
Configure an External Microsoft SQL Database

1 Logon to the Admin Console for the first cluster node.

2 Select **Cluster** > **Database** and click **Edit**.

3 Select **Microsoft SQL Server**.

4 Complete the following fields to configure your database:
   - **Database Host**: DNS name or IP Address of the SQL server
   - **Database Port**: 1433
   - **Database User**: SQL account created during initial SQL setup.
   - **Database Password**: Password set for the SQL account created during initial SQL setup.
   - **Database Name**: Name of the blank database created during initial SQL setup

5 Click **Save** to configure the database. A message confirms the setup has been successful.

6 Restore the backup of the appliance configuration you took prior to configuring clustering.

7 Select **Home** > **Status** to ensure that appliance is fully set up.
Configure the Appliance on the Initial Cluster Node

The following appliance settings from the initial cluster node are shared between appliances in the cluster:

- DNS server settings
- Certificate settings
- WINS settings
- Database configuration settings
- NTO server settings
- Web client enabled state
- DSCP setting
- Toggle Web Client setting
- HTTP Access setting
- Syslog settings
- Kerberos settings
- License details

It is recommended that, once you have enabled clustering and set up the database on the first node, you configure the appliance settings or restore a backup with the required settings configured. When further nodes are added to the cluster, the appliance settings are automatically applied.

Note
Application settings, such as Map Points, are not automatically moved to the SQL server when database settings are updated. A backup of the required settings must be restored to seed these settings in the database when switching from a configured local setup to a clustered one.

Check the Load Balancer Status

1. Select **Configuration > Advanced**.
2. Locate the Load Balancer Status section.

   ![Load Balancer Status](http://dnk.com:8001/status)

   Status URL: http://dnk.com:8001/status

   - Enable maintenance mode

   When this setting is enabled the server is temporarily removed from the load balancer pool. This setting has no effect unless the load balancer environment is configured to monitor the status URL.

   ![Update](http://dnk.com:8001/status)

3. Click the Status URL link to check the health status of a server in a load balanced environment. A status page is displayed showing one of the following:

   - **Success** - The server is functioning correctly within the load balancer pool.
   - **Failure** - The server is either offline or is not functioning correctly within the load balancer pool.
Configure Additional Cluster Nodes

Once you have successfully configured the initial cluster node, configure all the nodes you want to be part of the cluster.

1. Boot up the appliance for the node you are adding to the cluster.
2. Log in to the Admin Console for that node and Upload a License File.
3. On the appliance text console, press F2 and logon.
4. Select Cluster Configuration and press Enter.
5. Enter the name of the cluster. This must be the name you entered when setting up the initial cluster node.
6. If you are not using the standard port number (49152), enter the port number you are using for your cluster.
7. Press F10 to save the cluster configuration.
   If you have already performed configuration via other nodes of the cluster, the settings are automatically updated to any new nodes in the cluster and thereafter should automatically remain synchronised through updates when any setting changes.
8. Repeat this process for every new node that you add to the cluster.

Manage a Cluster in the Admin Console

If clustering is enabled on the appliance, you can check the status of the nodes in your cluster, apply a patch to your cluster, update, and shutdown nodes.

Patch Server

By nominating one of the nodes in a cluster as the Patch Server, you can apply patches to all nodes in the cluster. Any active node in a cluster can be used as the patch server.

To make a node the patch server, log into the web admin console for a node that is not currently the patch server, select Cluster > Status and click Promote to Patch Server. The current node is now identified as the patch server.
## Status

The status shows the name of the cluster, the DataNow server version, and which node in the cluster is currently the patch server.

### Cluster Status

The state of each node in the cluster is denoted by the icon displayed in the Cluster Status column.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="checkmark.png" alt="Active Icon" /></td>
<td><strong>Active</strong>&lt;br&gt;The node is online and using the correct DataNow server version, determined for the cluster by the version applied to the patch server.</td>
</tr>
<tr>
<td><img src="warning.png" alt="Warning Icon" /></td>
<td><strong>Warning</strong>&lt;br&gt;This can signify one of the following states:&lt;br&gt;&lt;ul&gt;&lt;li&gt;A patch server has not been set. Set one of the nodes as the patch server.&lt;/li&gt;&lt;li&gt;The node's DataNow server version is different to that of the patch server. Reapply the current patch to the cluster. This updates only those nodes that are not at the DataNow server version applied to the patch server. Nodes already at the correct version are unaffected by the update.&lt;/li&gt;&lt;li&gt;The node requires a reboot. Click the Reboot button for the node.&lt;/li&gt;&lt;li&gt;Component information cannot be retrieved.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td><img src="cross.png" alt="Inactive Icon" /></td>
<td><strong>Inactive</strong>&lt;br&gt;The node is offline.</td>
</tr>
</tbody>
</table>

If a patch server has not been set, these details are not displayed.
Host

Displays the name of each node in the cluster, identifies which node is the patch server, and which node you are currently accessing through the web admin console. Click on a name to see details of the current component versions of that node and its patching history. The name of the current node and the patch server are annotated appropriately.

<table>
<thead>
<tr>
<th>Host</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>dn-play-05</td>
<td>(this)</td>
</tr>
<tr>
<td>dn-play-01</td>
<td>(Patch Server)</td>
</tr>
<tr>
<td>dn-play-02</td>
<td></td>
</tr>
<tr>
<td>dn-play-04</td>
<td></td>
</tr>
</tbody>
</table>

IP Address

The IP address of each node in the cluster.

Action

In the web admin console for any node in the cluster, use the buttons in the Actions column to reboot or shutdown any other node in the cluster. If a node is inactive, it can be removed from the list using the corresponding button. If a removed node restarts, it will automatically re-display in the list.
Update

The Update screen displays cluster name, DataNow Server Version and which node is the current patch server. All patches that have previously been uploaded are listed in the Updates area.

Apply a Patch to a Cluster

This process explains how to apply a patch to all nodes in a cluster. To apply a patch when clustering has not been enabled, see Apply a DataNow Patch. You can apply a patch to a cluster using any nodes as long as one of the nodes in the cluster is the patch server. To make the current node the patch server, select Cluster > Status and click Promote to Patch Server.

1 Log into the web admin console on any node in the cluster.
2 Select Cluster > Update.
   In the Status section, details of the current patch version are displayed.
3 Click Choose File and navigate to a DataNow patch file.
4 Click Upload.
   The patch is displayed in the Updates section of the screen along with all patches that have been previously uploaded.

   Tip
   Select a patch and click Delete to remove it from the list and from the patch server.
5 Select the row in the table of the required patch and click Deploy Update.
   To see the components and release notes for a patch, click the patch name.
   Updates are applied in parallel to all components across the cluster that are not the same version as the patch. Nodes may require a reboot following an update - click Reboot in the Action column for the appropriate nodes. Nodes that are offline are not updated and display with a warning icon in the Status screen. Reapply the patch when the node is online to update its components. This does not affect any nodes that have already been updated.

The progress of the update is displayed and you are informed when the update is complete.
Advanced Configuration

The advanced options are used to set DSCP QoS options and to create and restore configuration backups. Select Configuration > Advanced to access the Advance options.

DSCP QoS Configuration

- Stays the same (link layer and routing protocol keep alive)
- Stays the same (used for IP routing protocols)
- Express Forwarding (EF)
- Class 4
- Class 3
- Class 2
- Class 1
- Best effort (QoS disabled)

This setting is only required if your organization uses Differentiated Services Code Point (DSCP) settings to help manage its network traffic.

The setting must be applied in accordance with your organization’s networking requirements. Your network team will be able to advise which setting to apply.

In the DSCP QoS Configuration area of the Advanced options, select the required configuration and click Update.

HTTP Access

- Enable access over HTTP

This should only be used in a load balanced environment or with an SSL offload appliance.

In the HTTP Access area of the Advanced options, configure the required setting and click Update to apply.

Caution

This option should only be used to enable connection by HTTP in a load balanced environment or with an SSL offload appliance.
NTP

Add the server addresses or FQDNs of the NTP servers you want to use. Insight is configured with the addresses of three default NTP servers. If you use your own NTP servers, replace the default addresses with the addresses of your own. You can use a maximum of three NTP servers and a minimum of one.

Load Balancer Status

Click the Status URL link to check the health status of a server in a load balanced environment. A status page is displayed showing one of the following:

- Success - The server is functioning correctly within the load balancer pool.
- Failure - The server is either offline or is not functioning correctly within the load balancer pool.

Enable Maintenance Mode

Select **Enable Maintenance Mode** to temporarily take the server offline. The server is no longer available in the load balancer pool and cannot be communicated with. This allows any necessary maintenance and configuration tasks to be completed. Whilst the server is in Maintenance Mode, the status of the server shows as ‘failure’.

De-select **Enable Maintenance Mode** to make the server available in the load balancer pool once again.

SMB Storage Authentication

Set the authentication method used by the DataNow appliance to connect to the SMB Storage - NTLM or Kerberos.
SMTP Configuration

Set up SMTP to use the required account for initiating Link Based Sharing emails.

**Caution**
The server URL, provided in the client’s request, is used to create the link included in emails to users. The DataNow server URL configured for your company’s appliances must be accessible externally.

1. Select **Configuration > Advanced**.

2. In the SMTP Configuration section, enter the details of the SMTP server and email address:
   - Hostname or IP address of the SMTP server
   - SMTP server port number
   - Encryption type to use when sending emails
   - The email address to send emails from
   - Email address to receive test email
   - Indicate if authentication is required and, if so, provide the username and password

3. Click **Update**.

Syslog Server

1. Select **Configuration > Advanced** and scroll down to the Syslog Server section of the screen.

2. Enter the IP address of the remote syslog server and click **Update**.
Policy

Configure a range of settings to determine how DataNow is used in your organization and by whom. There are four categories of policy rules in DataNow. Select Policy and the required category:

- **Global** - Set restrictions on platform, IP address, timeout and login attempts that apply to all your users.
- **Mobile** - Configure a range of settings to dictate how DataNow behaves on mobile devices.
- **Map Point Access** - Define policy settings unique to each map point allowing different sets of rules to match the requirements of different users and groups of users.
- **Users and Devices** - Verify new users and devices and manage their access. Users and devices can be remote wiped and unlocked if required.
Global Policy

Set restrictions on platform, IP address, timeout and login attempts that apply to all your users.
In the admin console, select Policy > Global and click Edit. When all required changes have been made, click Save.

Client Access

The table below illustrates this behavior.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Global</th>
<th>Map Point</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>On</td>
<td>On</td>
<td>Users for that Map Point can access the DataNow server through Windows.</td>
</tr>
<tr>
<td>Mac</td>
<td>On</td>
<td>Off</td>
<td>Users for that Map Point cannot access your server on a Mac as the Global setting is overridden.</td>
</tr>
<tr>
<td>iOS</td>
<td>Off</td>
<td>Off</td>
<td>Users cannot access your server on an iOS device regardless of their Map Point.</td>
</tr>
<tr>
<td>Android</td>
<td>Off</td>
<td>On</td>
<td>Users cannot access your server on an Android device regardless of their Map Point as the Map Point setting is overridden.</td>
</tr>
</tbody>
</table>
IP Address Login Restrictions

Specify which IP addresses can access your DataNow server using the following formats:
1. Separate a list of IP addresses with a comma or a space. For example, 22.12.144.220, 12.144.33.0.
2. Specify a range of values using a dash. For example, 222.12.144.220-255.
3. Use an asterisk to specify a wildcard - any value between 0 and 255. For example, 222.12.144.*

Failed Login Attempts

Set the number of consecutive failed login attempts before a user is locked out for the specified time period.
You can also specify the number of consecutive failed login attempts before locally stored data is wiped from the desktop or device.

**Note**
If an account is wiped in this way, the user is put on the Remote Wipe list for the web platform which prevents the user from all web login attempts.
It is therefore recommended that you do not set the failed login attempts before wiping data at a very low figure (less than five).

This policy works differently for mobile devices where the PIN check occurs on the local device, not the server. There is no lockout for PIN attempts but if the Remote Wipe setting does apply - if the number of PIN attempts exceeds the Remote Wipe Failed Login Attempts number, the local device is wiped of all data and stored login credentials, including the PIN.
Sharing

Set the length of time, in days, that files are available to recipients when shared by a link. If you do not require a time limit for a share, set to **Off**.

When updating this setting, changes only apply to newly created shares - existing shares adhere to the setting which was applied when the share was created.

**Note**
The figure set here is also the number of days a share is extended by when an expiry date is extended.
Mobile Policy

Configure a range of settings to dictate how DataNow behaves on mobile devices.

In the admin console, select Policy > Mobile and click Edit. When all required changes have been made, click Save.

Client Security

<table>
<thead>
<tr>
<th>Client Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store the user's encrypted password in the mobile device keychain.</td>
</tr>
<tr>
<td>If enabled, user may use a PIN for authentication instead of a password.</td>
</tr>
<tr>
<td>If disabled, the user must enter their password each time they launch the DataNow app.</td>
</tr>
<tr>
<td>☑ Require PIN authentication check every time DataNow app launches or returns to the foreground.</td>
</tr>
<tr>
<td>User must re-enter their password after 30 minutes of inactivity.</td>
</tr>
</tbody>
</table>

There following security policies are available:

- Set whether user’s encrypted passwords is stored in the mobile device keychain.
  - **On** - Users can use a PIN for authentication instead of a password.
  - **Off** - Users must enter their password each time they launch the DataNow app.

If this policy is enabled, a further option is available - **Require PIN authentication check every time DataNow app launches to the foreground**. If this policy is applied, users must enter their PIN each time the DataNow app launches or returns to the foreground.

- Set whether users must enter their password after a defined period of inactivity. This can be in minutes, days
Data Security

Set the DataNow behavior for downloaded files using the buttons to configure the following:

- **Wipe downloaded files** - Only stores files whilst they are in the foreground on a device. When the file is no longer in the foreground, the local copy is deleted from the device or endpoint.

- **Allow downloaded files to be opened by other apps** - Files downloaded from the DataNow app can be opened in other apps. This can potentially compromise security as files opened in other apps may be able to be printed or saved in a non-encrypted format.

- **Allow copy/pasting from the DataNow app to other apps** - Protect your organization’s sensitive information by disabling copy and paste from DataNow apps.

- **Allow file uploads** - Select whether users can upload files from their mobile devices to your DataNow server. When this option is set to On, it enables and disables the ‘Open in’ feature from other apps to DataNow. If this option is turned off, all downloaded files are read-only and users cannot upload files to your DataNow server.
Map Point Policy

Create and maintain policies, platform and file sharing options for map points. A policy can be created to define permissions for users connected to the map point. Further policies can be defined to set different permissions for individual users, Organizational Units (OU) and User Groups.

In the example below, one policy has been created for Admin Users and one for all other users. Admin Users can only connect to the server on verified devices whilst for all other users connected to the map point, all data is read-only. These policies apply concurrently on the map point.
Edit Map Point Access

1. Select **Policy > Map Point Access**.

   **Note**
   Map Point Access policy settings can also be accessed directly from the link in the corresponding map point connection string configuration - **Configuration > Map Points**.

2. Click **Edit**.

   ![Map Point Access Policy Settings](image)

   **Policies for All Users**:
   - Force read-only (files may not be modified).
   - Only allow VERIFIED devices to connect.

   **Platform Access**:
   - Allow Windows Access
   - Allow Mac Access
   - Allow iOS Access
   - Allow Android Access
   - Allow Web Client Access

   **File Sharing**:
   - Disabled
   - Read-only
   - Collaboration

3. Click **Add** to create the policy you want to define:
   - **Organizational Units** - Find the OU you want to add and click **Select**.
   - **User Groups** - Find a user group and click **Select**.
   - **Individual Users** - Find a user and click Add by the users you want to set a policy for.

4. Select an OU, User Group, Individual user or select **All Users** to apply settings to everyone who uses that map point.
5 Configure the required settings:

- **Force read-only** - Users cannot modify or upload DataNow files.

- **Only allow VERIFIED devices to connect** - Only those devices which have been approved by the administrator can connect to the DataNow server.

- **Platform Access** - Set which devices users can use to for this Map Point.

  Platform Access can also be set globally which can conflict the Map Point policy settings as show by the examples in the table below.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Global</th>
<th>Map Point</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>On</td>
<td>On</td>
<td>Users for that Map Point can access the DataNow server through Windows.</td>
</tr>
<tr>
<td>Mac</td>
<td>On</td>
<td>Off</td>
<td>Users for that Map Point cannot access your server on a Mac as the Global setting is overridden.</td>
</tr>
<tr>
<td>iOS</td>
<td>Off</td>
<td>Off</td>
<td>Users cannot access your server on an iOS device regardless of their Map Point.</td>
</tr>
<tr>
<td>Android</td>
<td>Off</td>
<td>On</td>
<td>Users cannot access your server on an Android device regardless of their Map Point as the Map Point setting is overridden.</td>
</tr>
</tbody>
</table>

- **Link Based Sharing** - Select whether the type of access internal and external users can have - either read-only or collaborative. Link based sharing can also be disabled.

6 Click **Save**.

These settings are applied to the users connected to the DataNow server who and match the defined criteria.
Users and Devices Policy

The Users & Devices page enables you to keep track of your users and their devices. The page shows you the users that have logged on to DataNow and displays details of each device on which they have installed DataNow. You can see the ID, type and status of all devices and have the option to verify any unverified devices. You can also remote wipe and unlock users and devices if necessary.

Search for Users and Devices

1. Select the **Policy** tab and click **Users & Devices**.
2. Select the required filters and enter your search criteria using the following filters:
   - **User/Device Status** - Display those users or devices at a particular status. For example, you might want to find all users who have been locked out or all unverified devices. Available options are:
     - All Users and Devices
     - Remote Wipe List Devices
     - Non-Remote Wipe Devices
     - Locked Out Users Only
     - Non-Locked Out Users
     - Verified Devices Only
     - Unverified Devices Only
   - **Platform Type** - Refine your list of devices by selecting a particular platform. For example, you might only want to view Android devices or Web Client sessions.
   - **User Name Matches** - Perform a search on full or part user names.
3. Click **Show Users/Devices** to update your user/device list using the filter and search settings.
Manage Users and Devices

1. Select a user(s) and/or device(s) - each user and device has their own checkbox.

2. Click the required action:

- **Remote Wipe User/Device** - All DataNow files are removed from the selected device or, if a user is selected, from all of their devices. This is useful for ensuring sensitive data is not left on a lost or stolen device or on the devices of someone who has left your organization. If a user is logged in at the time of the wipe, their next action on the device automatically returns to the login screen. The current session is invalidated and any login attempts are rejected.

- **Unlock User/Device** - If a user has had too many unsuccessful login attempts, their account is temporarily locked as defined in the Failed Attempts policy. Once unlocked, the failed login counter is reset.

- **Verify Device** - Any device that logs in for the first time is considered unverified until an admin manually approves/verifies the device in the DataNow appliance. Once verified, a device is added to the verified category and can only be removed following a remote wipe.

The action is performed for the selected devices and/or users.
Auditing

The DataNow appliance supports sending audit and usage data to a single remote syslog server over a TCP connection. The DataNow server requires the IP address and port of a remote syslog server. Only IP addresses are supported as DNS can be unreliable.

The syslog message contains JSON encoded data which can be indexed by software, such as Splunk, to provide reporting and analysis. The facility levels in syslog distinguish between usage and audit log data as follows:

<table>
<thead>
<tr>
<th>Level</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>local2</td>
<td>audit data</td>
</tr>
<tr>
<td>local3</td>
<td>usage data</td>
</tr>
</tbody>
</table>

All messages are sent at the informational severity level.

Configure a Remote Syslog Server in DataNow

1. Select Configuration > Advanced and scroll down to the Syslog Server section of the screen.
2. Enter the IP address of the remote syslog server and click Update.
Set up a Remote Syslog Server

The syslog server must be configured to listen on a TCP port for it to work with DataNow. The following steps instruct you how to do this using either Rsyslog or Splunk.

Rsyslog

The standard syslog service included in Ubuntu Server is Rsyslog.

1. Create a DataNow configuration file in the /etc/rsyslog.d folder called 10-dnsyslog.conf.
2. Add the following lines to 10-dnsyslog.conf to listen for TCP traffic on port 10514:
   
   # provides TCP syslog reception
   $ModLoad imtcp
   $InputTCPServerRun 10514

3. To filter out the DataNow messages to separate log files you must create a directory /var/log/datanow and ensure that the syslog daemon has permission to write to that directory.
4. Add the following lines to 10-dnsyslog.conf to redirect the DataNow messages and stop them appearing in the normal syslog files:
   
   local2.* /var/log/datanow/audit.log
   &~
   local3.* /var/log/datanow/usage.log
   &~

5. Restart the syslog server to pick up changes using the following command:
   
   service rsyslog restart

Splunk

These instructions apply to Splunk Enterprise 5 on Linux.

2. Download splunk.tar which contains the DataNow configuration for Splunk.
3. Untar the files on the Splunk server and copy inputs.conf, props.conf and transforms.conf to $SPLUNK_HOME/etc/system/local directory.
   
   $SPLUNK_HOME refers to the directory where Splunk is installed. If these files are already present then merge them with the existing files.
4. Restart Splunk using $SPLUNK_HOME/bin/splunk restart

   Splunk should now be listening on Port 10514 for syslog traffic.
5. Configure the DataNow appliance to point at the Splunk server IP address.
Troubleshooting

Check for data arriving on the Syslog server

Check for data arriving on the syslog server either in /var/log/syslog or var/log/datanow/usage.log using the following tail command:

```
tail -f /var/log/datanow/usage.log
```

Check the server is listening

On the syslog server, use the following command to ensure the server is listening on the port configured:

```
netstat -nlt | grep 10514
```

The response should be:

```
tcp 0 0 0.0.0.0:10514 0.0.0.0:* LISTEN
```

Check the DataNow appliance has connected

On the syslog server, use the following command to ensure the DataNow appliance has connected:

```
netstat -nt | grep 10514
```

The response should be:

```
tcp 0 0 [syslogserver]:10514 [datanow appliance]:42901 ESTABLISHED
```

If support mode is enabled on the DataNow server and you have SSH access, then running netstat on the DataNow server should show a similar connection as above.
Report Logs

You can download configuration reports and appliance logs which can be used by AppSense support to check your installation, performance and to troubleshoot your appliance.

Select **Home > Status** and click the download link.

You may be asked for these reports when contacting AppSense about DataNow.
Install Trusted Certificates

To use an enterprise certification authority (CA), you need to install the enterprise root SSL certificate on each of the client devices. The instructions in this chapter provide information designed to help you install root certificates on Windows, Mac, iOS and Android clients. Network provisioning tools are also available for installing trusted SSL certificates on clients. However, these instructions focus on individual clients.

You only need to add a root certificate to client devices if the enterprise is using a private CA. If you experience difficulties with a certificate issued by a public CA then review the appliance certificate configuration.

Note
For testing purposes during the evaluation phase of your DataNow deployment, to avoid installing the default self-signed certificate on each client device, it is recommended that you request a free time-limited certificate from one of the public CAs.

Install Root Certificates on Windows

Web browsers and the DataNow Client use the operating system certificate store. So, if you install the certificate in the operating system then both the DataNow Client and Internet Explorer automatically trust the server certificate.

This procedure describes one method of installing the root certificate using Internet Explorer and Microsoft Management Console on Windows 7.

1. In Internet Explorer, browse to the DataNow Website or DataNow Admin Console as follows:
   - Website: https://<server_address>
   - Admin Console: https://<server_address>
   The browser displays a security warning.

2. Click Continue to the website.

3. In the address bar, right-click the certificate and select View Certificates.

4. On the certificate dialog, click the Details tab.

5. Click Copy to file.

6. In the wizard, select Base-64 encoded binary X.509 (.CER).
   The saved file contains the certificate. You can view the file in a text editor to see the certificate.

   Note
   The certificate must be installed as a trusted certificate for the computer. To do this, run the Microsoft Management Console (MMC) as administrator and add the Certificates snap-in. If MMC is run as a standard user, trusted certificates can only be added at the user account level.

7. Click the Windows Start button.

8. In the search box, begin typing mmc.exe, right-click the mmc.exe entry in the search results and select Run as Administrator.

10 Select **Certificates** and click **Add**.

11 In the Certificates snap-in dialog, select **Computer account** and complete the wizard.

12 Click **OK**.

13 In the MMC console, expand **Certificates**.

14 Right-click **Trusted Root Certificates** and select **All Tasks > Import**.

15 Follow the Certificate Import Wizard to import the certificate.

After installing the certificate, close and reopen Internet Explorer and load the DataNow Website or DataNow Admin Console. If the certificate installed correctly and is valid, the security warning no longer displays.

### Install Root Certificates on Mac

Both the web browser and the DataNow Client use the operating system certificate store. So, if you install the certificate in the operating system using Safari then the DataNow client automatically trusts the certificate.

This procedure describes installing the root certificate on a Mac OS X 10.7.3 using Safari 5.1.3.

1. Launch Safari and browse to the DataNow Website or DataNow Admin Console as follows:
   - Website: https://<server_address>
   - Admin Console: https://<server_address>
   - Safari displays a message, “Safari can’t verify the identity of the website”.

2. Click **Show Certificates**.

3. Select, when using this certificate, **Always Trust**.

   The Secure Sockets Layer (SSL) and X.509 Basic Policy trusts update to Always Trust.

4. Click **Continue**.

5. Provide your password and click **Update Settings**.

Safari adds the root certificate to the certificate store and the browser starts trusting the server.
Install Root Certificates on Android

This procedure is based on installing the root certificate on a Google Nexus phone running Android 4.0.4. It uses Internet Explorer in Windows 7 to download the certificate. You need to connect the phone to the PC using a USB cable in order to transfer the file to the device. For other phones you can use removable memory cards or email to transfer the file.

1 Connect the phone to the PC using a USB cable.

2 In Internet Explorer, browse to the DataNow Website or DataNow Admin Console as follows:
   - Website: https://<server_address>
   - Admin Console: https://<server_address>
   The browser displays a security warning.

3 Click **Continue to the website**.

4 In the address bar, right-click the certificate and select **View Certificates**.

5 On the certificate dialog, click the **Details** tab.

6 Click **Copy to file**.

7 In the wizard, select **Base-64 encoded binary X.509 (.CER)** and save the file locally on the PC.
   You must install this certificate as a trusted certificate for the Android device.

8 Copy the file to the root of the Android internal storage.
   **Note**
   For the Google Nexus this is **Computer > Galaxy Nexus > Internal Storage**.

9 Disconnect the phone from the PC.

10 On the phone, pull down the status bar and click the settings button beside the date.

11 Select **Security > Credential storage > Install from storage**.

12 Verify the certificate name and click **OK**.
   Android adds the certificate to the phone trusted certificates.
Install Root Certificates on iOS

This procedure is based on using the provisioning tool, iPhone Configuration Utility 3.5, on Windows 7 to create or edit a configuration profile containing the certificate and to provision it to an iPad or iPhone. As an alternative, you can email the certificate file to the device and install it. Configuration profiles are XML files that contain device security settings including certificates.

**Note**
To install the certificate on an iOS device, first install the certificate in the computer operating system - either Windows or Mac.

1. In iPhone Configuration Utility, select **Configuration Profiles**.
2. Select an existing profile or click **New** in the toolbar to create one.
3. At the top of the list, click **General** and complete the form.
4. Further down the list, click **Credentials**.
5. If Credentials are not configured, click **Configure**, otherwise, click the plus symbol to add a certificate.
   A dialog displays the certificates installed on the computer operating system.
6. Select the required certificate.
7. Plug your iOS device into the computer.
8. In the Devices list, click the device name.
9. Click the **Configuration Profiles** tab.
10. Select the profile you edited, and click **Install**.

   The iPhone Configuration Utility installs the configuration and certificates on the device.
Roll Out DataNow

After configuring DataNow, all end users specified in the MS Active Directory below the Base DN have access to the website and can synchronize their home folders using the DataNow client. Users now need to know how DataNow helps them, where to download the client, the address of the DataNow appliance and how to use DataNow on their devices.

1. Store the client downloads in an accessible location ready for download by users. Consider selecting a location that is accessible from inside and outside the enterprise firewall.

2. If you use AppSense Application Manager software consider elevating user rights for the DataNow installer.

3. Communicate the following suggested details to end-users:
   - How and where to download the Windows and Mac clients.
   - How to install the Android clients from the Google Play app store
   - (search for AppSense).
   - How to install the iOS client for iPhone and iPad from the iTunes app store (search for AppSense).
   - The server address, username and password to use in the client
   - (their usual username and password from MS Active Directory).
   - How to visit the appliance website using a secure https connection.

   **Tip**
   The server address for the client and the website address are the same.

   - Links to the DataNow Help Center:
   - Your support arrangements in case they encounter difficulties.
   - Links to the enterprise acceptable usage policy.
   - If you are not using a Public CA, the details of the enterprise SSL certificate and instructions.
Using a Private or Enterprise Certification Authority

We recommend that you use a public Certification Authority (CA). However, your organization might use an Enterprise CA and a private CA for proof of concept (PoC) tests.

The following procedure describes generating certificates using Microsoft Enterprise Certificate Authority on Windows Server. Other Enterprise CA solutions are available.

If you are not using a public CA you need to install the root certificate for your private CA on the appliance before installing any chain certificates and the appliance certificate. You also need to provision the root certificate on every client device that uses the DataNow client.

Request a Certificate Using a Microsoft Private CA

1. In a web browser, navigate to:
   https://<your CA>/certsrv
2. Click Request a Certificate.
3. Click Advanced certificate request.
4. Click Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or Submit a renewal request by using a base-64-encoded PKCS #7 file.
5. Paste the CSR you generated into the Saved Request field.
6. From the Certificate Template list, select Web Server and click Submit.
7 Select **Base 64 encoded**, click **Download certificate chain** and save.

8 Once the download is complete, install the certificates and follow the processes detailed in:

   a  Prepare your certificates

   b  Apply a certificate to the DataNow appliance
DataNow SAN Certificates

This section provides information about configuring a DataNow certificate that contains SANName entries.

Subject Alternative Name (SAN) extensions allow a certificate subject to be associated with the service name and domain name components of a DNS Service Resource Record. This enables us to publish multiple DNS names using one SSL web listener.

This allows administrators to use CNAME alias DNS records with an SSL certificate that has a different Common Name set within the subject of the certificate.

This document assumes that you have a functioning DataNow appliance with a base DNS, AD, admin user and license configuration applied already.

The configuration is in three parts, DNS, General Certificate and DataNow Appliance.

DNS and SAN Certificates

1. Create DNS entries for your appliance.

   - mddn1 Host (A) 10.70.22.174
   - DataNowExternal Alias (CNAME) MDDN1.mbd.support.local

2. Check that both records resolve correctly.

![Ping command output]

H:\> ping mddn1
Pinging mddn1.MBD-support.local [10.70.22.174] with 32 bytes of data:
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64

Ping statistics for 10.70.22.174:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms

H:\> ping DataNowExternal
Pinging mddn1.MBD-support.local [10.70.22.174] with 32 bytes of data:
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64

Ping statistics for 10.70.22.174:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 1ms, Average = 0ms

H:\>
General Certificate

1. Open Microsoft Management Console.
2. Select **Add Certificates > Computer account > local computer.**
3. Click **Finish** and **OK.**
4. Expand Personal and select **Certificates.**
5. Right-click in the center pane and select **Request New Certificate.**
   The Certificate Enrollment wizard displays.
6. Click **Next** and **Next** again.
7. Select **Web Server** and click **Properties.**

The Certificate Properties options are displayed.
8 Complete the following fields in the Subject name options.

- Common Name
- Organizational Unit
- Organization
- Locality
- State
- Country
- Email

This would be the same information you enter into the DataNow appliance when generating a CSR request.
9. In the Alternative name section, select **DNS** from the Type drop down.

10. In the Value field, add the Alternative DNS names to be included in the certificate request.

11. Select the General tab and enter a Friendly Name and optional Description.
12 Select the Private Key tab and expand the Key Options.

13 Select **Make private key exportable**.

14 Click **Apply** and **OK**.

15 In the Certificate Enrollment dialog, click **Enroll**.
16 When the certificate has successfully enrolled, click **Finish**.

You should see the certificate in the Personal store.

![Certificate in Personal store](image)

17 Right-click on the new certificate and select **Open**.

18 Click on the Details tab and select **Subject**.

You will see the subject details for your certificate.

![Certificate Details](image)
19 Scroll to the **Subject Alternative Name** section.

The alternative DNS names you configured should be visible.

```plaintext
DNS Name=mdln1.mbd.support.local
DNS Name=mdln1
DNS Name=datanowexternal.mbd.support.local
DNS Name=datanowexternal
```

Learn more about [certificate details](#)
20 Click **Copy to File** and then **OK**.

21 Click **Next**.

22 Enable the **Yes, export the private key option** and click **Next**.
23 In the export file format section, select **Include all certificates in the certification path possible** and click **Next**.

![Certificate Export Wizard](image)

- **Export File Format**
  - Certificates can be exported in a variety of file formats.

  - Select the format you want to use:
    - **DEA encoded binary X.509 (.CER)**
    - **Base 64 encoded X.509 (.CER)**
    - **Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)**
      - Include all certificates in the certification path if possible
    - **Personal Information Exchange - PKCS #12 (.PFX)**
      - Include all certificates in the certification path if possible
      - Delete the private key if the export is successful
      - Export all extended properties
    - **Microsoft standards Certificate Store (.PST)**

  Learn more about [certificate file formats](#).
24 Type and confirm a password and click **Next**.
25 Save the certificate to a suitable location.
26 Complete the wizard by clicking finish.
SAN Certificates in the DataNow Appliance

1. Open a web browser and connect to your Appliance Admin console.
2. Select Configuration > SSL Certificate.

   ▼ If you have an existing certificate you’d like to use
   
   Upload a PKCS #12 or PFX certificate file (.p12 or .pfx file extension).
   
   Browse

   Encryption Password used to create file: [Enter password]

   [Upload Certificate]

3. Click Browse and select the required certificate.
4. If the certificate was created with an encryption password, type it into the field provided.
5. Click Upload Certificate and your certificate should be installed and enrolled for the host name you specified in the Certificate Subject.

You should now be able to use the A and CNAME record to connect to the appliance using SSL.

'A' Record Connection example

![A Record Connection example](image1)

'CNAME' Record Connection example

![CNAME Record Connection example](image2)